3/2019

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

42. Jahrgang
ISSN 0137-7767
12,00 Euro

Real Time Bidding

■ Real Time Bidding – die Versteigerung der Internet-User ■ #FixAdTech – Verhaltenskodizes nach Artikel 40 DSGVO für Online-Werbung ■ Beschwerde wegen VERHALTENSBASIERTER WERBUNG im Internet ■ Online-Werbung reparieren – für Journalismus und Grundrechte ■ Ahnenforschung mit Gendaten ■ Offener Brief an die EU-Kommission ■ Nachrichten ■ Rechtsprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt



Termine

Samstag, 26. Oktober 2019
DVD-Vorstandssitzung
Bonn

Sonntag, 27. Oktober 2019
DVD-Mitgliederversammlung
Bonn

Freitag, 01. November 2019
Redaktionsschluss DANA 4/2019
Minderjährigen(Daten)schutz
(Arbeitstitel)

Freitag, 27. bis Montag, 30. Dezember 2019
36C3 - 36. Chaos Communication Congress
Leipzig

Foto: Pixabay..com

DANA

Datenschutz Nachrichten

ISSN 0137-7767

42. Jahrgang, Heft 3

Herausgeber

Deutsche Vereinigung für Datenschutz e.V. (DVD)

DVD-Geschäftstelle:

Reuterstraße 157, 53113 Bonn

Tel. 0228-222498

IBAN: DE94 3705 0198 0019 0021 87

Sparkasse KölnBonn

E-Mail: dvd@datenschutzverein.de

www.datenschutzverein.de

Redaktion (ViSdP)

Dr. Thilo Weichert

c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)

Reuterstraße 157, 53113 Bonn

dvd@datenschutzverein.de

Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz

Frans Jozef Valenta, 53119 Bonn

valenta@datenschutzverein.de

Druck

Onlineprinters GmbH

Rudolf-Diesel-Straße 10

91413 Neustadt a. d. Aisch

www.diedruckerei.de

Tel. +49 (0) 91 61 / 6 20 98 00

Fax +49 (0) 91 61 / 66 29 20

Bezugspreis

Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

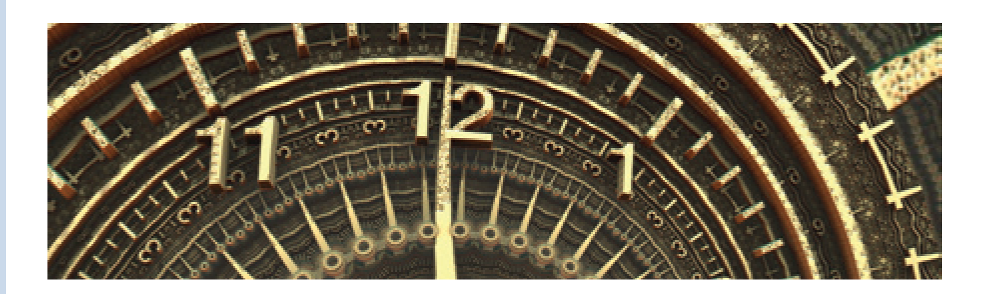
Leserbriefe

Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos

Frans Jozef Valenta, Pixabay

Editorial



Ursprünglich plante der DVD-Vorstand, für das vorliegende Heft den „Datenschutz für Kinder und Jugendliche" zum Schwerpunkt zu nehmen. Das Thema ist schon lange relevant und steht weiterhin auf der Liste unserer Planungen. Doch legten aktuelle Entwicklungen es nahe, mit dem „Real Time Bidding" ein anderes Thema in den Fokus zu stellen. Die von Liberties gestartete europaweite Kampagne zum Versteigern von personalisierter Internet-Werbung wird in Deutschland neben der DVD von Digitalcourage, der Digitalen Gesellschaft und dem Netzwerk Datenschutzexpertise mitgetragen. Die vorliegende DANA versteht sich als ein Teil dieser Kampagne, mit der Licht in das dunkle Feld der Internet-Finanzierung sowie der im Hintergrund stattfindenden Datenflüsse geschaffen werden soll.

Ein weiterer Schwerpunkt dieser DANA-Ausgabe ist die genetische Ahnenforschung. Hierzu hat Ende 2018 das Netzwerk Datenschutzexpertise ein umfangreiches Gutachten veröffentlicht, das aber von den Medien, den Betroffenen und den beteiligten Stellen weitgehend ignoriert wurde. Dies änderte sich schlagartig, als AncestryDNA im Juni 2019 den BigBrotherAward in der Kategorie Biotechnologie verliehen bekam. Das Thema wird kontrovers diskutiert. Doch anders als beim Real Time Bidding sehen die Betreiber der Angebote sowie deren Protagonisten (noch) keine Veranlassung, sich mit den Aufsichtsbehörden oder mit einer kritischen Öffentlichkeit in einen direkten Diskurs zu begeben. Während die kritische Öffentlichkeit das Geschäftsmodell der Werbeverwendung von Internetdaten in Frage stellt, scheint dies bei der Vermarktung von Gendaten noch nicht der Fall zu sein. Umso wichtiger ist es, hierüber aufzuklären.

Wie gewohnt enthält diese Ausgabe wieder viele Nachrichten aus der Welt des Datenschutzes von nah und fern sowie aktuelle einschlägige Gerichtsentscheidungen.

Viel Erkenntnis und Spaß beim Lesen! Rückmeldungen an die DANA-Redaktion bzw. den DVD-Vorstand sind immer willkommen.

Thilo Weichert

Autorinnen und Autoren dieser Ausgabe:

Friedemann Ebelt
DigitalCourage e. V., friedemann.ebelt@digitalcourage.de

Markus Eßfeld
Vorstandsmitglied in der DVD, essfeld@datenschutzverein.de

Elisabeth Niekrenz
Digitale Gesellschaft e. V., elisabeth.niekrenz@digitalegesellschaft.de

Frank Spaeing
Vorstandsmitglied in der DVD, spaeing@datenschutzverein.de

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Thilo Weichert

Real Time Bidding - die Versteigerung der Internet-User

Das Realitätsbewusstsein und die Realität selbst liegen in kaum einem Bereich so weit auseinander wie bei der Internet-Datenverarbeitung. Hinter einer mit farbigen bewegten Bildern illustrierten Oberfläche findet eine Verarbeitung unserer Daten statt, von der selbst ExpertInnen oft keine genaue Vorstellung haben. Und es gibt kaum einen Bereich, in dem das reale „Ist" so weit vom rechtlichen „Soll" abweicht wie hier. Ein Beispiel hierfür ist das Real Time Bidding (RTB), das durch die Veröffentlichung des Berichts von Johnny Ryan vom 05.09.2018 erstmals öffentlich thematisiert wurde.[1] Dieser Bericht wurde im Herbst 2018 die Grundlage erster Beschwerden bei der irischen und der britischen Datenschutzbehörde. Diese Beschwerden sind die Blaupause für mehrere am 04.06.2019 europaweit eingereichte Beschwerden im Rahmen einer von „Civil Liberties for Europe" initiierten europaweiten Kampagne. Mit der seit Mai 2018 direkt anwendbaren Datenschutz-Grundverordnung (DS-GVO) besteht ein europaweit einheitliches Instrument zur Hinterfragung der mit dem Begriff „Real Time Bidding" beschriebenen Praktiken.

- Das Phänomen

Was bedeutet Real Time Bidding (RTB), auf deutsch „Echtzeitversteigerung"? Dahinter verbirgt sich eine spezifische Art der Vermittlung von personalisierter Online-Werbung, bei der Internet-Werbeplätze jeweils demjenigen Werbetreibenden zugeschlagen werden, der das höchste Zahlungsgebot macht. Oder in den Worten des in diesem Bereich tätigen Bundesverbands Digitale Wirtschaft e. V. (BVDW): „Realtime Bidding benennt den Prozess eines automatisierten Preisfindungsverfahrens in Form einer Auktion. Werbetreibende legen ihre Zahlungsbereitschaft für eine zur Verfügung stehende Werbeeinblendung – in Kombination mit weiteren Informationen wie z. B. Nutzerdaten oder auch den Kontext – im Rahmen eines Gebots fest. In der folgenden Auktion haben sie die Möglichkeit, diese Werbeeinblendung zu ersteigern, stehen dabei allerdings im Wettbewerb mit anderen Werbetreibenden. Die Bewertung der Werbeeinblendung durch den Werbetreibenden und die Abgabe des Gebots erfolgt in Echtzeit. Arten des Realtime Biddings sind First Price Auction oder Second Price Auction." Bei First Price Auctions zahlt der Höchstbietende den von ihm gebotenen Preis. Bei der Second Price Action zahlt der Höchstbietende den Preis des zweithöchsten Gebots.[2]

Praktiziert wird diese Versteigerung insbesondere von Google sowie von weiteren Online-Anbietern, die sich im IAB Europe zusammengeschlossen und hierüber gemeinsame Standards festgelegt haben. IAB steht für „Interactice Advertising Bureau". Zu den 18 Mitgliedsländern des IAB Europe gehören neben Deutschland Belgien, Dänemark, Finnland, Frankreich, Griechenland, Großbritannien, Italien, Kroatien, Niederlande, Norwegen, Österreich, Polen, Rumänien, Schweden, Slowenien, Spanien und die Türkei. Der Verband wird zudem durch 20 Unternehmensmitglieder getragen. IAB Europe hat seinen Sitz in Brüssel. Seine deutschen Mitglieder sind organisiert im Online-Vermarkterkreis (OVK). Unter dem Dach des Bundesverbands Digitale Wirtschaft (BVDW) haben sich darin 18 der größten Online-Vermarkter zusammengeschlossen, um ihre gemeinsamen Interessen zu vertreten. Dabei handelt es sich um Scout24 Media, Bauer Media Group, Burda Forward, ebay advertising, G+J e/MS, himedia digital advertising experts, IP Deutschland, iq digital, MairDumont Netletix, media impact, netpointmedia, OATH, Otto group media, SevenOneMedia, Spiegel Media AdAlliance, Ströer, united internet media.

Informations-, Kommunikations- und Service-Angebote im Internet erfolgen in einem großen Maße unentgeltlich. Oft erfolgt die Refinanzierung solcher Angebote über personalisierte Werbung. Letztlich basiert das Geschäftsmodell vieler Internet-Angebote darauf, dass diese sich von den Usern nicht mit Geld, sondern mit den kommerziell verwertbaren Nutzerdaten „bezahlen" lassen. So sind die Daten der Nutzenden die Grundlage für das Anzeigen und die Bepreisung personalisierter Werbung. Jedes Anzeigen einer Werbung kostet das werbende Unternehmen einen kleinen Geldbetrag. Um hier eine möglichst wirksame Investition zu tätigen, wollen die Werbenden möglichst zielgerichtete Werbung. Diese setzt voraus, dass die Werbewirtschaft die Internetnutzenden kennt. Dem dient das „Profiling", also das Erstellen von Nutzerprofilen. Mit detaillierten Profilen soll eine möglichst große Response erreicht werden, insbesondere durch den Kauf von beworbenen Produkten. Ob die Werbung dadurch wirkt, dass sie einem bestimmten Nutzerprofil entspricht, wird zumeist automatisiert festgestellt. Auch der Abgleich des Werbeintention mit dem Nutzerinteresse erfolgt durch einen Algorithmus. Das werbende Unternehmen kann hierfür die erwünschten Merkmalseigenschaften der zu Bewerbenden festlegen. Auch dieser Prozess ist zumeist automatisiert.

Beim Profiling beschränkt sich die Werbeindustrie nicht auf die Adressierung des Endgeräts. Das Profiling zielt vielmehr auf die sich hinter dem Endgerät vermuteten Nutzenden. Diese werden mit Cookies, device-, browser- oder canvas-fingerprinting erkannt und dies auch geräteübergreifend (cross-device tracking). Die Festlegung der Werbeadressaten wird zumeist vollständig Algorithmen überlassen. Menschen mit verschiedenen digitalen Profilen bekommen beim Besuch der gleichen Webseite und zur gleichen Zeit regelmäßig unterschiedliche, nämlich personalisierte Werbung angezeigt. Beim RTB erfolgt nicht nur die Vermittlung von Werbung an einen Werbeanbieter, sondern auch die Preisfestlegung über Algorithmen.

Die folgende Darstellung der konkreten Abläufe von RTB basiert weitgehend auf dem Bericht des Information Commissioner´s Office (ICO) „Update report into adtech und real time bidding“ vom 20.06.2019. Das ICO ist die britische Datenschutzaufsichtsbehörde. Der Webseiten- oder Applikationsbetreiber versucht demnach beim RTB aus jeder Werbeanzeige den größtmöglichen Preis herauszuhandeln. RTB kann zum Einsatz kommen auf Informationsportalen, einfachen Webseiten, aber auch beim Audio- oder Videostreaming, im Rahmen von Online-Spielen oder jedem sonstigen Internet-Angebot – für stationäre wie für mobile Endgeräte. Hierzu startet der Webseiten- oder Diensteanbieter eine Gebotsanfrage (Bid request), die an das RTB-Ökosystem übermittelt wird, wobei diese Anfrage in der Regel personenbezogene Daten des Nutzenden enthält. Die aktuelle Profilbildung, die Generierung der Gebotsanfrage, die Versteigerung, der Zuschlag und letztlich die Anzeige der Werbung erfolgen innerhalb weniger Millisekunden, so dass dem Nutzenden seinem Profil angepasste Anzeigen präsentiert werden. Die Standards für die Abwicklung dieser Prozesse werden von Google in dessen „Authorized Buyers Real Time Bidding“ oder von IAB im OpenRTB in Protokollen festgelegt. Die in das RTB-Ökosystem eingebundenen Stellen können die über die Gebotsanfrage erlangten Daten mit Angaben aus eigenen oder anderen Quellen anreichern (data matching, enrichment), wobei diese Angaben sowohl personenbezogen wie auch aggregiert sein können.

Am RTB sind nicht nur die Werbefirmen (advertisers) und die Anbieter (publishers) beteiligt. Vielmehr sind weitere Beteiligte zwischengeschaltet. Das sind zunächst die Vermittler (advertising exchanges), auf deren Plattform die Werbeangebote und Werbeanfragen zusammengeführt und die Höchstbieter ausgewählt werden. Dann gibt es Data Management Platforms (DMPs), die aus verschiedenen Quellen einlaufende Datensätze sowohl aus den Gebotsanfragen wie aus den Werbeanfragen analysieren, kategorisieren und zusammenführen. Andere Plattformen organisieren die Werbung verschiedener Unternehmen (Demand Side Platforms – DSPs), wieder andere organisieren die Angebote der Dienstebetreiber (Supply Side Platforms – SSPs). Schließlich ist es denkbar, dass bei einwilligungsbasierter Werbung Dienstleister zwischengeschaltet werden, die die Werbeanfragen mit dem Einwilligungsumfang der Nutzenden vergleichen und freigeben (Consent Management Platforms – CMPs).

Die Qualität und der Umfang der Gebotsanfragen kann unterschiedlich sein; in der Regel enthalten sie folgende Merkmale: Identifikator der Gebotsanfrage, (evtl. verkürzte) IP-Adresse, Cookie-IDs, Nutzer-IDs, Browser, Gerätetyp und -art, Nutzerlokalisierung, Zeitzone, Sprache, sowie weitere variable individuelle oder aggregierte Nutzerinformationen. Es handelt sich dabei um personenbezogene Informationen, die teilweise eine direkte, teils nur eine indirekte Zuordnung zu einer konkreten Person ermöglichen. Die Zuordnung kann durch den Empfänger der Gebotsanfrage dadurch erfolgen, dass bei ihm schon Merkmalsdaten des Nutzenden zumindest über ein Pseudonym zuordenbar vorliegen. Bei den zusätzlichen Nutzerinformationen kann es sich um Angaben über das Surfverhalten (vorherige, nächste Seite), den Clickstream oder sonstige Vorgehensweisen auf einer Seite handeln, um Angaben über Suchanfragen, Nutzungszeiten, Inhaltsangaben oder demografische Informationen.

So enthält das IAB „content taxonomy“ Hunderte verschiedener Felder, beispielsweise zu „Herz- und Kreislaufkrankheiten“, „psychische Gesundheit“, „sexuelle Gesundheit“, „ansteckende Krankheiten“. In Googles „publisher verticals“ finden sich die Merkmale wie „Fortpflanzungsfähigkeit“, „Drogenmissbrauch“, „Gesundheitsbedingungen“, „Politik“ und „ethnische und andere Gruppenidentitäten“. Bei vielen der übermittelten Merkmale handelt es sich um sog. sensitive Daten, deren Verarbeitung grundsätzlich verboten ist und nur unter engen Voraussetzungen, im Bereich der Werbung nur durch „ausdrückliche Einwilligung“, erlaubt wird (Art. 9 Abs. 2 lit. a DSGVO). Die Merkmale können so dafür genutzt werden eine Werbeanzeige vorzunehmen oder diese zu verhindern.

Es kommen beim RTB insbesondere zwei Protokolle zur Anwendung: 1. das „OpenRTB Protokoll“ des IAB evtl. in Verbindung mit dem „Transparency and Consent Framework“ (TCF) des IAB Europe, 2. Googles „Authorized Buyers Framework“. Diese technischen Spezifikationen beschreiben präzise, welche Daten bei den Übermittlungen ausgetauscht werden und wie der Austausch stattfindet. Die Protokolle zielen auf eine Standardisierung unabhängig von den Marktteilnehmern ab. Es gibt weitere, teilweise mit OpenRTB kompatible Protokolle.

Die Gebotsanfrage wird an eine Vielzahl von Empfängern weitergeleitet. Dabei kann es sich um Hunderte, ja Tausende von Empfängern handeln. Die Empfänger erhalten diese Daten, ohne dass es wirksame Vorkehrungen gibt, um deren weitere Verarbeitung zu verhindern oder zumindest zu beschränken.

- Rechtliche Bewertung

Die datenschutzrechtliche Bewertung des RTB erfolgt auf der Grundlage des Telekommunikationsrechts und der DSGVO. Gemäß Art. 95 ist die DSGVO im Anwendungsbereich der europäischen Telekommunikations-Datenschutzrichtlinie (TK-DSRl) nicht anwendbar. Die TK-DSRl soll frühestmöglicht durch die im Gesetzgebungsprozess befindliche europäische ePrivacy-Verordnung ersetzt werden. Die TK-DSRl wird im nationalen Recht im vorliegenden Bereich durch das Telemediengesetz (TMG) umgesetzt. Zwar bestehen Unsicherheiten, inwieweit das TMG im Bereich des Datenschutzes nach Wirksamwerden der DSGVO anwendbar ist. Unstreitig ist aber, dass die Regelungen des TMG nicht zu unterschreitende Mindeststandards festlegen. Soweit eine Umsetzung der TK-DSRl durch das TMG nicht erfolgt ist, kommt deren direkte Anwendbarkeit in Betracht. Dies gilt insbesondere für Art. 5 Abs. 3 TK-DSRl, der für den Einsatz von Cookies für Werbezwecke eine Einwilligung verlangt. Das TMG beschreibt klare Anforderungen an die Information bzw. Anzeigen gegenüber den Betroffenen (§§ 13 Abs. 1, 4, 15 Abs. 2 S. 2 TMG), die sich u. a. auf den Einsatz von Identifikatoren, Datenweiterleitungen, die Einschaltung von Stellen außerhalb der EU und die verfolgten Zwecke beziehen müssen. Hinsichtlich elektronisch erteil-

ter Einwilligungen bestehen ebenso klare Anforderungen (§ 13 Abs. 22, 3 TMG).

Art. 9 Abs. 1 DSGVO verbietet die Verarbeitung personenbezogener Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen, ebenso von Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung. Eine Nutzung solcher Daten für Werbezwecke ist nur ausnahmsweise erlaubt, wenn der Betroffene unter Benennung der Verantwortlichen und des konkreten Zwecks „ausdrücklich einwilligt" (Art. 9 Abs. 2 lit. a DSGVO). Diese Voraussetzungen sind beim RTB durchgängig nicht gegeben. So stellte das britische ICO fest, dass die Verarbeitung derartiger Daten über das RTB unzulässig ist.[3]

Hinsichtlich der Verarbeitung von nichtsensitiven Daten gilt Art. 6 Abs. 1 DSGVO. Zwar ist generell anerkannt, dass Werbung ein berechtigtes Interesse begründen kann (Art. 6 Abs. 1 lit. f DSGVO). Doch muss die konkrete Verarbeitung für den Zweck erforderlich sein. Eine Erforderlichkeit der Übermittlung der Daten an Hunderte und mehr Empfänger im Rahmen einer Gebotsanfrage ist für den Zweck der Werbeeinblendung nicht gegeben, so dass auch bzgl. nichtsensitiver Merkmale der Vorgang unzulässig ist, soweit nicht eine Einwilligung erteilt wird (Art. 6 Abs. 1 lit. a DSGVO). Hinzu kommt, dass eine Abwägung mit den Interessen der Betroffenen erfolgen muss. Eine solche Abwägung ist bisher – soweit erkennbar – in den Protokollen bei Google und des IAB Europe nicht vorgesehen. Schließlich müsste den Betroffenen eine wirksame Möglichkeit eines Widerspruchs und des Ausschlusses vom RTB gegeben werden (Art. 21 DSGVO, § 15 Abs. 3 TMG). Es erfolgt hierüber, obwohl verpflichtend vorgesehen (Art. 21 Abs. 2-4 DSGVO, § 15 Abs. 3 S. 2 TMG), auch keine Information. Die technischen Voraussetzungen für eine Umsetzung von Widersprüchen sind regelmäßig nicht vorhanden.[4]

Eine Einwilligungsnotwendigkeit ist gemäß Art. 5 Abs. 3 TK-DSRl auch in Bezug auf die Verarbeitung von Cookie-Daten gegeben, die beim RTB weit verbreitet ist. Eine Einwilligung setzt eine gewisse Bestimmtheit bzgl. der verarbeiteten Daten wie der Empfänger voraus. Diesen Anforderungen wird beim RTB nicht genügt.

Die Art. 13, 14 DSGVO machen es erforderlich, dass die Betroffenen über Empfänger oder zumindest Kategorien von Empfängern, über die verfolgten Zwecke, über Drittlandsübermittlungen sowie über weitere Aspekte informiert werden. Drittlandsübermittlungen sind im Rahmen des RTB üblich, insbesondere bei Angeboten von Google sowie anderen US-Unternehmen. Entsprechende Informationspflichten bestehen auch nach dem TMG (s. o.). Die gesetzlich geforderte Transparenz wird beim RTB nicht hergestellt.

Art. 5 Abs. 2 DSGVO verlangt von den Verantwortlichen, dass diese die Einhaltung ihrer Pflichten nach der DSGVO, insbesondere der in Art. 5 Abs. 1 DSGVO normierten Grundsätze, nachweisen können. Tatsächlich sind weder die Protokolle von Google noch die von IAB Europe in der Lage, den im dem RTB-Ökosystem beteiligten Stellen Klarheit über ihre Verantwortlichkeit zu geben.

Beim RTB erfolgt in den meisten Fällen ein umfassendes Profiling der Betroffenen. Dieses verstößt gegen Art. 22 DSGVO, der umfassende Sicherungsmaßnahmen zugunsten der Betroffenen fordert.[5] Diese sind nicht ersichtlich. Selbst wenn man die Ansicht vertreten würde, dass das einfache Anzeigen von Online-Werbung keine von Art. 22 DSGVO erfasste Entscheidung ist, handelt es sich bei den Profilingmaßnahmen, auf deren Grundlage RTB durchgeführt wird, um unverhältnismäßige, unfaire Eingriffe in das Persönlichkeitsrecht der Betroffenen.[6]

Gemäß Art. 25 DSGVO müssen bei der Technikgestaltung die Grundsätze des Privacy by Default und Privacy by Design realisiert werden. § 13 Abs. 4 TMG verlangt zugunsten der Nutzenden darüber hinausgehende und konkretisierende Vorkehrungen. Weder bei Google noch in den Vorgaben von IAB Europe sind Verfahren festgelegt, mit denen diese Prinzipien auch nur im Ansatz umgesetzt würden. Art. 32 DSGVO verpflichtet zudem zum Ergreifen einer Vielzahl von Sicherheitsmaßnahmen. Diese betreffen nicht nur die eigene Datenverarbeitung, sondern auch den Empfang und die Übermittlung von Daten. Beim RTB erfolgen Übermittlungsketten, in deren Verlauf – soweit ersichtlich – bisher keine Sicherungsmaßnahmen etabliert sind.

Bei RTB handelt es sich um Verarbeitung mit einem hohen Risiko für die Rechte und Freiheiten der Betroffenen. Es erfolgt eine systematische und umfassende Bewertung persönlicher Aspekte einschließlich der umfangreichen Verarbeitung sensitiver Daten. Bei derartigen Verfahren ist eine umfassende Datenschutz-Folgenabschätzung (Art. 35 DSGVO) gefordert. Es ist nicht erkennbar, dass die am RTB beteiligten Stellen diesen Anforderungen genügen, ja dass sie diese Anforderungen überhaupt erkannt haben.

- Konsequenzen

Aus der obigen Darstellung ergibt sich zwingend, dass die aktuelle RTB-Praxis unzulässig ist. Zu diesem Ergebnis kommt auch die britische Datenschutzaufsichtsbehörde, das ICO. Sie stellt fest, dass Tausende von Organisationen jede Woche im Vereinigten Königsreich Milliarden von personenbezogenen Gebotsanfragen verbreiten ohne angemessene technische und organisatorische Sicherungsmaßnahmen und ohne Rücksicht auf die Beschränkungen z. B. bei Drittlandsübermittlungen.[7] Diese Feststellung hat Gültigkeit für die gesamte Europäische Union (EU). Als Maßnahme hat das ICO bisher insbesondere vorgesehen, weitere Fakten über das RTB zu sammeln. Die wesentlichen Beteiligten sollen gezielt angesprochen und zum Dialog veranlasst werden. Dabei ist eine enge Zusammenarbeit mit den anderen Datenschutzbehörden in der EU angestrebt. Diese ist ohnehin nach der kollektiven, von Civil Liberties koordinierten Beschwerde-Initiative vom Juni 2019 notwendig. Das ICO kündigte eine weitere Bestandsaufnahme innerhalb von sechs Monaten an. Bis dahin soll die Werbeindustrie ihr RTB-Ökosystem selbst umfassend neu bewerten. Das ICO versäumt es dabei nicht darauf hinzuweisen, dass RTB nur ein Teil eines umfassenderen Datenschutzproblems personalisierter Online-Werbung darstellt.

Angesichts der Fakten und der vernichtenden rechtlichen Bewertung ist es auf den ersten Blick geradezu er-

schreckend, wie defensiv das ICO mit seinen „Maßnahmen“ agiert. Die Möglichkeiten des Art. 58 Abs. 2 DSGVO gehen bis zum Totalverbot, die des Art. 83 Abs. 6 DSGVO bis zu Bußgeldern in Höhe von maximal 4% des „gesamten weltweiten erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres“. Es war bisher nicht erkennbar, dass von Seiten der Verantwortlichen bei Google, des IAB Europe sowie der RTB-Unternehmen konkrete Maßnahmen ergriffen wurden oder werden, die auch nur im Ansatz geeignet sind, rechtskonforme Zustände herzustellen.

Tatsächlich kann das Ergebnis mittelfristig nur ein völliges Verbot des RTB sein. Dem könnte sich die Industrie nur dadurch entziehen, dass sie umgehend Systeme aufsetzt, bei denen das Ersteigern von Werbeplätzen von folgenden engen Stellschrauben abhängig gemacht wird: Verzicht auf sensitive Merkmale oder Kategorien, Aggregierung zu Merkmalsgruppen, die das Profiling beschränken, Zulassung von maximal einem Identifikator, umgehende Löschpflicht nach Abschluss des jeweiligen Auktionsvorgangs, Verbot der Datenanreicherung, Transparenz für alle Beteiligten, insbesondere für die Betroffenen, Einräumung des Widerspruchsrechts, Information der Betroffenen hierüber und über dessen technische Umsetzung, technisch-organisatorische Vorkehrungen, die eine zweckwidrige Datennutzung in der Verarbeitungskette wirksam verhindern. Die Erfahrungen mit dem Wirtschaftszweig begründen die berechtigte Befürchtung, dass diese Zielvorgaben nicht akzeptiert werden. Nur wenn mit diesen Zielvorgaben und einem klaren engen Zeitplan vorgegangen würde, wäre es vertretbar, kurzfristig die milliardenfachen Verletzungen des Datenschutzrechtes zu tolerieren.

Die Aufsichtsbehörden müssen sich zweifellos innerhalb der EU und insbesondere im Europäischen Datenschutzausschuss zu dem Thema verständigen (Art. 63 ff. DSGVO). Sie sollten sich aber schon jetzt auf ein Szenario einstellen, das auf Verbote und höchstmögliche Geldbußen hinausläuft. Dabei ist es wichtig, dass bei der Auswahl der Adressaten die bestimmenden Unternehmen als erste in den Fokus genommen werden. Dazu gehört zweifellos Google. Datenschutz sollte und darf keine verdeckte Diskriminierung im Wettbewerb bewirken. Daher ist es nötig, auch die weiteren großen außereuropäischen und die europäischen Unternehmen in den Fokus zu nehmen. Hierfür ist zweifellos noch einiges an Sachverhaltsaufklärung nötig. Doch sind die Fakten zu eindeutig, als dass nicht sofortiges planvolles Vorgehen unumgänglich ist, das letztlich auf ein vollständiges Verbot dieser Vorgehensweise hinausläuft.

1 Report from Dr. Johnny Ryan – Behavioural advertising and personal data, https://brave.com/Behavioural-advertising-and-personal-data.pdf; Übersetzung hiervon in diesem Heft S. 133.

2 https://www.bvdw.org/glossar/.

3 Informations Commissioner´s Office (ICO), Update report into adtech and real time bidding, 20 June 2019, S. 16.

4 benso ICO S. 18.

5 Weichert in Däubler/Wedde/Weichert/Sommer, EU-Datenschutz-Grundverordnung und BDSG-neu, 2018, Art. 22 DSGVO Rn. 31f.

6 ICO S. 20.

7 ICO S. 23.

Elisabeth Niekrenz

#FixAdTech – Verhaltenskodizes nach Artikel 40 DSGVO für Online-Werbung

Mit der EU-weiten Beschwerdekampagne #StopSpyingOnUs fordern die beteiligten Datenschutz- und Menschenrechtsorganisationen von den Datenschutzaufsichtsbehörden die umfassende Überprüfung eines verbreiteten Vertriebsmodells für personalisierte Werbung – Real Time Bidding. Daneben schlagen sie die Ausarbeitung von Verhaltensregeln gemäß Art. 40 DSGVO für personalisierte Werbung vor. Was macht die von der DSGVO vorgesehenen Verhaltenskodizes aus und weshalb ist ein solcher Kodex für das gesamte Feld von Online-Werbung notwendig?

Personalisierte Werbung wurde etwa in den letzten zehn Jahren zu einer bestimmenden Einnahmequelle für Webseitenbetreibende, insbesondere für Presse- und sonstige Medienunternehmen, die Medienprodukte online zur Verfügung stellen und regelmäßig eine Vielzahl von Webseitenbesuchern verzeichnen. Den Vertrieb ihrer Werbeplätze nehmen sie nicht durch einzelne Verträge mit Werbekunden vor, sondern sie gliedern sich oftmals an eines der beiden europaweit meistverbreiteten Real Time Bidding-Systeme an – Google Authorized Buyers bzw. Open RTB. Für letzteres ist maßgeblich das Interactive Advertisement Bureau (IAB) verantwortlich, das auch das zugehörige Transparency and Consent Framework aufstellt. Die beteiligten Unternehmen verstoßen in diesem Rahmen umfangreich und systematisch gegen geltendes Datenschutzrecht. Für Webseitenbetreibende stehen wenige Angebote zum datenschutzkonformen Vertrieb von Werbeplätzen zur Verfügung. Diese strukturellen Datenschutzverstöße sollten durch strukturelle Maßnahmen angegangen werden. Gerade weil sich die DSGVO auf einem hohen Abstraktionsniveau bewegt und einiger Konkretisierung durch die Rechtsprechung

bedarf, sollte die europäische Werbebranche europaweit gültige Verhaltensregeln für die Datenverarbeitung bei Online-Werbung formulieren und diese den Datenschutzaufsichtsbehörden zur Genehmigung vorlegen. Solche Verhaltensregeln müssen freilich grundlegende Veränderungen der derzeit verbreiteten Vertriebsmodelle vornehmen.

Real Time Bidding: eine problematische Struktur

Das IAB stellt auf seiner Website technische Spezifikationen des Open RTB-Systems zur Verfügung. Der europäische Ableger, das IAB Europe hat zudem am 25.04.2018 das Transparency and Consent Framework veröffentlicht.[1] Es handelt sich um ein Regelwerk, das gewährleisten soll, dass die Einwilligung zur Datenverarbeitung, die eine Person dem Webseitenbetreiber gewährt, für sämtliche Datenweitergaben an Dritte gilt, obgleich der ursprüngliche Verantwortliche die Kontrolle über die Daten vollständig verliert, sodass eine Information der Nutzerinnen und Nutzer über die weitere Verwendung und damit eine informierte Einwilligung systematisch verunmöglicht wird.[2] Wie die weiteren Glieder dieser Ketten Daten verarbeiten, etwa an wen sie sie weitergeben oder ob sie Profile über Menschen erstellen, ist unkontrollierbar. Den betroffenen Nutzerinnen und Nutzern ist es faktisch nicht möglich, diese Verarbeitungen nachzuvollziehen oder ihre Rechte nach der DSGVO, etwa auf Auskunft oder Löschung, gegenüber den einzelnen Instanzen geltend zu machen.

Der Kontrollverlust über die Datenverarbeitung ist durch die Protokolle und Regelwerke der Branche nicht nur normativ, sondern auch technisch determiniert. Deshalb ist es nur folgerichtig, eine Überprüfung dieser Strukturen zu verlangen. Es liegt an der Branche selbst, insbesondere am IAB Europe als deren Verband, datenschutzkonforme Spielregeln zu schaffen und sie den Aufsichtsbehörden zur Genehmigung vorzulegen.

Verhaltenskodizes nach Art 40 DSGVO

Die Genehmigung von Selbstregulierungsinstrumenten war bereits nach altem Recht in § 38 BDSG a.F. vorgesehen, davon wurde in der Vergangenheit aber nur sehr eingeschränkt Gebrauch gemacht.[3] Gemäß Art. 40 Abs. 1 DSGVO fördern die Datenschutzaufsichtsbehörden die Ausarbeitung von Verhaltensregeln, die die Verordnung für bestimmte Wirtschaftsbereiche konkretisieren. Ihrem Förderauftrag können die Behörden etwa dadurch nachkommen, dass sie Verbände zum Verfassen solcher Regelungen ermutigen und dabei beratend zur Seite stehen.[4] So soll den Spezifika verschiedener Branchen durch Selbstregulierung Rechnung getragen werden.[5] Während etwa die Zertifizierung (Art. 42 DSGVO) konkrete Datenverarbeitungsvorgänge konkreter Verantwortlicher betrifft, sollen mit Verhaltenskodizes allgemeine Regeln für ganze Geschäftsfelder geschaffen werden.[6]

Gemäß Art. 40 Abs. 2 DSGVO können Branchenverbände solche Regelungen ausarbeiten und der zuständigen Datenschutzbehörde zur Genehmigung vorlegen. Es handelt sich mithin um eine „regulierte Selbstregulierung“: Die Normen dürfen das Schutzniveau der DSGVO nicht unterschreiten.[7] In einem solchen Fall müsste die zuständige Behörde die Genehmigung verweigern. Sofern die betroffenen Datenverarbeitungen mehrere Mitgliedsstaaten betreffen, gibt gemäß Art. 40 Abs. 7 DSGVO auch der Europäische Datenschutzausschuss (EDSA) eine Stellungnahme im Kohärenzverfahren gemäß Art. 63 DSGVO ab.

Was den Inhalt betrifft, so können alle Bereiche der DSGVO durch Verhaltenskodizes konkretisiert werden. Art. 40 Abs. 2 lit. h i.V.m. Art. 24 Abs. 1 DSGVO sieht dies insbesondere für technische und organisatorische Maßnahmen vor, die die Einhaltung des Datenschutzrechts sicherstellen sollen. Zwingend müssen Regeln zur Überwachung der Einhaltung des Kodex durch eine dafür vorgesehene Stelle vorhanden sein.

Die Mitglieder des Verbandes sind nicht automatisch in der Pflicht, sich an einen Verhaltenskodex zu halten. Die im Einzelnen verantwortlichen Unternehmen können sich vielmehr freiwillig zur Einhaltung verpflichten. Dies bewirkt zwar nicht per se, dass sämtliche darauf basierenden Datenverarbeitungen rechtmäßig sind.[8] Die Selbstverpflichtung kann aber dazu dienen, die Einhaltung von Pflichten gemäß Art. 24 Abs. 3 (Erfüllung der Verantwortung), Art. 28 Abs. 5 (Garantien des Auftragsverarbeiters) oder Art. 32 Abs. 3 DSGVO (Sicherheit der Verarbeitung) zu belegen bzw. Nachweiserleichterungen herbeizuführen.[9] Sie erlangen zudem Bedeutung für eine Datenschutz-Folgenabschätzung, für die Übermittlung von Daten ins Ausland und schließlich für den relevanten Bereich der Bußgeldverhängung (Art. 83 Abs. 2 lit. j DSGVO), sind also durchaus geeignet, ein gewisses Mehr an Rechtssicherheit im Umgang mit den abstrakten Bestimmungen der DS-GVO zu schaffen.

Besonders relevant ist, dass Art. 40 Abs. 9 DSGVO der Kommission die Möglichkeit eröffnet, eine Allgemeingültigkeitserklärung zu erlassen. Die Folge dieser Erklärung ist in der Literatur umstritten. Überwiegend wird vertreten, dass sie unmittelbare Wirkung für und gegen Jedermann entfaltet.[10] Das würde bedeuten, dass sämtliche Unternehmen, die im geregelten Bereich arbeiten, an diese Regelungen gebunden wären. Demnach könnte der Branchenkodex, wenn er von der Kommission für allgemeingültig erklärt wird, auch unmittelbare Auswirkungen auf die Beteiligten an Googles proprietärem System haben. So ließen sich Wettbewerbsnachteile für datenschutzkonform agierende Unternehmen vermeiden.

Fazit

Von der Verletzung der Privatsphäre aller Nutzenden des Internets ganz abgesehen, haben Fachleute aus der Werbebranche die Nachteile der AdTech-Industrie, die auf Tracking basiert, längst dargestellt: Nicht nur büßen Werbetreibende Seriosität ein, weil viele Nutzerinnen und Nutzer das Gefühl haben, von ihnen ausspioniert zu werden. Die Branche hat auch maßgeblich zu negativen Effekten für Gesellschaft und Demokratie beigetragen: Das Geschäftsmodell schafft vor allem Anreize, Inhaltsangebote zu kreieren, die durch aufsehenerregende Überschriften häufig aufgerufen werden und schafft damit eine materielle Voraussetzung von Klickbaiting und Fake News.[11] Inwiefern datenschutzkonforme Formen personalisierter Werbung mög-

lich sind könnte die Branche – durch die Aufsichtsbehörden beraten – erarbeiten. Solange personalisierte Werbung darauf basiert, das Surfverhalten von Personen an eine Vielzahl von Unternehmen zu übermitteln, ist dies jedenfalls nicht gewährleistet.

Neben der Verhängung von Bußgeldern gegenüber einzelnen Verantwortlichen, die durch Abschreckung Wirkung auf die gesamte Branche entfalten können, aber nicht müssen, würde die Erarbeitung eines Verhaltenskodexes mit einer Veränderung der entsprechenden Protokolle für einen grundlegenden Wandel der Branchenpraktiken auf einen Schlag sorgen, insbesondere, wenn der Kodex von der Kommission für allgemein gültig erklärt werden würde.

1 Abrufbar unter https://iabeurope.eu/tcfdocuments/documents/legal/currenttcftncFINAL.pdf.

2 Rn. 11, 12 des Beschwerdetextes.

3 Wolff, Verhaltensregeln nach Art. 40 DSGVO auf dem Prüfstand, ZD 2017, 151.

4 Ebd.

5 Lepperhoff, Gola, Datenschutz-Grundverordnung 2. Auflage 2018, Art. 40 Rn 1.

6 Jungkind, BeckOK Datenschutzrecht, Wolff/Brink 28. Edition Stand: 01.02.2019 Art. 40 Rn 6.

7 Lepperhoff, Gola, Datenschutz-Grundverordnung 2. Auflage 2018, Art. 40 Rn 1.

8 Jungkind, BeckOK Datenschutzrecht, Wolff/Brink 28. Edition Stand: 01.02.2019 Art. 40.

9 Lepperhoff, Gola, Datenschutz-Grundverordnung 2. Auflage 2018, Art. 40 Rn 5.

10 Vgl. Wolff, Verhaltensregeln nach Art. 40 DSGVO auf dem Prüfstand, ZD 2017, 151, 153.Vgl. zum Streitstand Jungkind, BeckOK Datenschutzrecht, Wolff/Brink 28. Edition Stand: 01.02.2019 Art. 40 Rn. 32.

11 Vgl. etwa: Doc Searl's Webblog: GDPR will pop the adtech bubble, 12.05.2018, abrufbar unter: https://blogs.harvard.edu/doc/2018/05/12/gdpr/.

Digitale Gesellschaft e. V./Netzwerk Datenschutzexpertise/Deutsche Vereinigung für Datenschutz e. V./Digitalcourage e. V.

Beschwerde bei den deutschen Datenschutz-Aufsichtsbehörden wegen VERHALTENSBASIERTER WERBUNG im Internet

und Aufforderung, hierzu Datenschutzleitlinien zu erarbeiten und zu veröffentlichen

A. Einführung & Zweck

1 Wir erheben in Absprache mit weiteren Organisationen in Europa die unten stehende Beschwerde. Wer wir sind:

- Die Digitale Gesellschaft e.V. ist ein gemeinnütziger Verein, der sich seit seiner Gründung im Jahr 2010 für Grundrechte und Verbraucherschutz im digitalen Raum einsetzt.
- Das Netzwerk Datenschutzexpertise ist ein Zusammenschluss von DatenschutzexpertInnen mit dem Ziel, öffentliche Diskussionen über Fragen des Datenschutzes sowie generell des Schutzes von Menschenrechten und Grundrechten in der digitalen Welt zu initiieren und voranzubringen.
- Die Deutsche Vereinigung für Datenschutz e. V. (DVD) nimmt seit ihrer Gründung 1977 als gemeinnütziger Verein die Interessen der verdateten BürgerInnen wahr.
- Digitalcourage e. V. ist ein Zusammenschluss von Menschen, die Technik und Politik mit dem Ziel der Verwirklichung von Grundrechten und Datenschutz kritisch erkunden und menschenwürdig gestalten wollen.

2 Der Zweck der vorliegenden Beschwerde ist es, die deutschen Datenschutzaufsichtsbehörden um Maßnahmen zu bitten, welche den Einzelnen bzw. die Menschen allgemein vor weitreichenden und systematischen Datenschutzverstößen durch Google und andere Internet-Unternehmen der Branche schützen. Die Beschwerde hat als Grundlage die Stellungnahme von Dr. Johnny Ryan (**Ryan-Bericht**).[1]

3 Es gibt zwei Hauptsysteme, die der verhaltensbasierten Online-Werbung zugrunde liegen, die beide nach einer Spezifikation namens „Real Time Bidding" (RTB) arbeiten:

- **OpenRTB** wird von praktisch jedem bedeutenden Unternehmen in der Online-Medien- und Werbebranche verwendet.
- **„Authorized Buyers"** ist Googles proprietäres RTB-System, das vor Kurzem von „DoubleClick Ad Exchange" (kurz „AdX") in „Authorized Buyers" umbenannt wurde.

4 Beide Systeme dienen dazu, personalisierte Werbung auf Websites bereitzustellen. Wie im Ryan-Bericht dargestellt, werden „jedes Mal, wenn eine Person auf eine Webseite geht, die automatisierte Werbung nutzt, und diese

herunterlädt, persönliche Daten über sie an Dutzende – oder gar Hunderte – von Firmen übertragen".

5 Es gibt drei zentrale, miteinander zusammenhängende Gründe für erhebliche Datenschutzbedenken beim Einsatz von verhaltensbasierter Internetwerbung.

Erstens Die Branche begann ursprünglich damit, personalisierte Werbung zu unterstützen. Inzwischen führt dies zu einer Übertragung von Massendaten, die

a ein breites Spektrum an Informationen über Einzelpersonen umfasst, welches weit über den Bereich der Informationen hinausgeht, der für die Bereitstellung der relevanten Anzeigen erforderlich ist, und

b einer Vielzahl von Dritten für eine Reihe von Anwendungen zur Verfügung gestellt werden, die weit über die Zwecke hinausgehen, welche eine betroffene Person verstehen kann und in die sie einwilligen oder gegen die sie Widerspruch einlegen kann. Es gibt keine rechtliche Grundlage für eine solche allgegenwärtige und invasive Profilerstellung und Verarbeitung personenbezogener Daten aus Profitgründen (Art. 22 Datenschutz-Grundverordnung – DS-GVO).

Zweitens Der praktizierte Mechanismus der Branche ermöglicht es nicht, die Kontrolle über die Verbreitung personenbezogener Daten nach deren Übertragung (bzw. überhaupt) zu behalten. Die schiere Anzahl der Empfänger solcher Daten führt dazu, dass die Sender weder ihre unbefugte Weiterverarbeitung verhindern, noch die betroffenen Personen über die Empfänger der Daten ordnungsgemäß informieren können. Die rechtskonforme Verarbeitung der personenbezogenen Daten kann nicht mehr gewährleistet werden, wenn diese einmal weitergegeben worden sind. Die technischen und organisatorischen Sicherheitsvorkehrungen, die getroffen wurden, bestätigen, dass Datenschutzverletzungen dem Design der Branche inhärent sind. Dieses Problem besteht unabhängig davon, ob die Verarbeitung personenbezogener Daten und der Informationsaustausch im Rahmen der personalisierten Werbung durchgeführt werden. Eine Verarbeitung ohne ausreichende Sicherheitsvorkehrungen ist mit den Datenschutzbestimmungen nicht vereinbar.

Drittens Die Verarbeitung betrifft sehr oft besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO). Die besuchten Webseiten können Indikatoren enthalten, die über Sexualität, Ethnizität, politische Meinungen etc. Auskunft geben. Solche Aussagen, die als sensitive Daten anzusehen sind, können explizit erfolgen oder effektiv und leicht mit hoher Genauigkeit unter Verwendung moderner analytischer Techniken abgeleitet werden.[2] RTB erfolgt in Echtzeit, was zur Folge hat, dass solche sensitiven Daten ohne jegliches Einverständnis und ohne jegliche Kontrolle verbreitet werden können. Da solche Daten mit sehr hoher Wahrscheinlichkeit an zahlreiche Organisationen weitergegeben werden, die diese Daten wiederum mit anderen Daten verknüpfen, können extrem komplexe Profile von Personen erstellt werden, ohne dass die betroffene Person davon Kenntnis hat, geschweige denn ihr Einverständnis gegeben hätte. Die Industrie fördert diese Praxis und verzichtet auf adäquate Sicherheitsmechanismen, welche die Integrität der persönlichen Daten und auch solcher besonderer Kategorien gewährleisten könnten. Darüber hinaus ist es unwahrscheinlich, dass Einzelpersonen wissen, dass ihre persönlichen Daten auf diese Weise verbreitet und übertragen wurden, es sein denn, sie sind aus einem speziellen Grund in der Lage, bei einer Vielzahl von Unternehmen erfolgreiche Anträge auf Zugang zu persönlichen Daten zu stellen.[3] Es ist nicht zu erkennen, dass diese Unternehmen solchen Anfragen nachgekommen sind und dass dies nachweisbar wäre. Ohne Maßnahmen der Regulierungsbehörden ist es nicht möglich, die branchenweite Einhaltung der Datenschutzbestimmungen sicherzustellen.

6 Angesichts dieser anhaltenden Verstöße gegen die einschlägigen Vorschriften und Gesetze werden die Datenschutzaufsichtsbehörden um Folgendes ersucht:

i Überprüfen Sie die detaillierten Beschwerdegründe, die hier und im Ryan-Bericht aufgeführt werden, und leiten Sie eine Untersuchung der speziellen Probleme in Bezug auf die Branche für verhaltensorientierte Werbung ein. Um gegen sie vorgehen zu können, ist es wichtig, die systematische Natur der in diesen Beschwerden aufgeführten Verstöße anzuerkennen.

ii Leiten Sie eine breit angelegte Untersuchung zu den Datenschutzpraktiken der Branche ein. Wir fordern die Datenschutzaufsichtsbehörden auf, ihre Befugnisse nach Kapitel VII der Europäischen Datenschutz-Grundverordnung (DS-GVO) auszuüben, um in Zusammenarbeit mit anderen Datenschutzbehörden eine gemeinsame Untersuchung der genannten Geschäftspraktiken durchzuführen. Wie im Folgenden näher ausgeführt, wurden entsprechende Beschwerden bereits bei Datenschutzbehörden anderer EU-Mitgliedstaaten eingereicht.

iii Darüber hinaus ersuchen wir die Datenschutzaufsichtsbehörden, die in dieser Beschwerde aufgeführten systematischen und weit verbreiteten Probleme und Bedenken gemäß deren gesetzlichen Auftrag nach § 40 Bundesdatenschutzgesetz (BDSG) zu untersuchen und eine Bewertung durchzuführen, ob die Branche die einschlägigen Datenschutzvorschriften einhält. Darüber hinaus fordern wir die Datenschutzaufsichtsbehörden auf, im Rahmen ihres Ermessens eine gemeinsame Prüfung der Branche vorzunehmen und geeignete Verhaltensregeln / Empfehlungen in Anlehnung an Art. 57 Abs. 1 lit. g, h DS-GVO zu erarbeiten und, falls erforderlich, Durchsetzungsmaßnahmen zu ergreifen.

7 Die von den Datenschutzaufsichtsbehörden geforderten Maßnahmen sind in den nachstehenden Ziffern 48 - 53 ausführlich beschrieben.

B. Hintergrund

8 Der Hintergrund der Branche ist in dem beigefügten Bericht von Dr. Ryan

(Ryan-Bericht) dargestellt. Wir verweisen die Datenschutzaufsichtsbehörden für eine detaillierte Erklärung zur Branche, zu deren Vorgehensweise und zu den dem System innewohnenden Datenschutzbelangen auf diesen Bericht.

C. Richtlinien und Verfahren

9 Die Unternehmen sind in einem Branchenverband zusammengeschlossen, der Parameter und Anwendungsmuster festlegt: das Interactive Advertising Bureau (IAB). Die europäische Niederlassung des IAB, **IAB Europe**, hat mit der „Industry Standard Policy" Verhaltensregeln und standardisierte Vorgehensweisen für Europa festgelegt. Wegen der marktbeherrschenden Stellung von Google handelt dieses Unternehmen mit *Authorized Buyers* nach eigenen Verfahren und Vorgehensweisen. Wir gehen nacheinander auf beides ein.

i. IAB Europe

10 IAB Europe hat das „Europe Transparency & Consent Framework" geschaffen (Framework).[4] Dieser Rahmen basiert auf der Idee, im Verlauf des RTB-Prozesses die Einwilligung von einer betroffenen Person für alle späteren Datenweitergaben an Dritte einzuholen.

11 Mit dem Design des Systems ist ein grundlegender Fehler verbunden. Das Framework erkennt ausdrücklich an, dass der für die Datenverarbeitung Verantwortliche, der „data controller" (und damit auch die betroffene Person), unmittelbar jede Kontrolle über die Verwendung dieser Daten verliert, sobald die Daten einer natürlichen Person übertragen wurden. Tatsächlich akzeptiert das Framework, dass selbst für den Fall, dass ein Empfänger von Daten gegen Gesetze verstößt, diesem Empfänger weiterhin Daten zur Verfügung gestellt werden dürfen.[5] Durch den Verzicht der „data controller" auf die Kontrolle verzichtet die Branche insgesamt darauf, den Anschein eines Mechanismus aufrechtzuerhalten, in dem es eine Rolle spielt, wie die Daten verwendet werden. Einmal abgegeben, ist die Kontrolle über diese Daten im Äther des Datenhandels für immer verloren.

12 Diese Daten werden dann an ein umfangreiches Ökosystem von Data Brokern und Werbetreibenden weitergegeben. Diese Dritten können die Daten dann nach eigenem Ermessen verwenden, wobei die Betroffenen als die „Datensubjekte" keinerlei Mitsprache, Kenntnis oder Kontrolle über diese nachfolgende Nutzung haben. Die Anwendungen für diese Daten sind umfangreich; sie können mit anderen Daten zusammengeführt werden oder die Daten können verwendet werden, um für viele unterschiedliche Zwecke ein Profil der betroffenen Person zu erstellen. Die letztliche Verwendung dieser Daten kann daher Bereiche umfassen, die vom ursprünglich Verantwortlichen in seiner Interaktion mit dem Kunden nicht erwähnt wurden. Solche Endverwendungen können für die betroffenen Personen bedenklich sein, wenn sie überhaupt davon Kenntnis erlangen.[6] Tatsächlich gibt es keine Möglichkeit für den Verantwortlichen, alle möglichen Endanwendungen zu erwähnen, da diese nach der Übertragung der Daten nicht mehr in seiner Macht stehen. Dieses Problem ist dem Design der Branche inhärent.

13 Darüber hinaus können die zu verarbeitenden Daten, wie im Bericht von Dr. Ryan beschrieben, besondere Kategorien personenbezogener Daten, sog. sensitive Daten, enthalten. Dass solche Daten ohne jegliche Kontrolle weitergegeben werden, ist äußerst problematisch.

14 Ein weiteres Problem dieses Frameworks liegt darin, dass es darauf abzielt, die Kontrolle über personenbezogene Daten nach deren Übertragung zu beseitigen. Das Framework geht davon aus, dass diejenigen, die solche personenbezogenen Daten verbreiten, sie auch ohne Einwilligung der Betroffenen an Dritte weitergeben.

Das Framework besagt (Betonung nicht im Original): *„Ein Anbieter kann sich aus einem beliebigen Grund dafür entscheiden, keine Daten an einen anderen Anbieter zu übermitteln, aber ein Anbieter darf keine Daten an einen anderen Anbieter übermitteln, ohne dass eine* ***gerechtfertigte Grundlage für die Annahme*** *vorliegt, dass der Verkäufer über eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten verfügt. Hat oder erhält ein Anbieter personenbezogene Daten und liegt keine Rechtsgrundlage für den Zugang zu diesen Daten und deren Verarbeitung vor, sollte der Verkäufer die Erhebung und Speicherung der Daten schnellstmöglich einstellen und von einer Datenweitergabe an andere Parteien auch dann absehen, wenn diese Parteien eine Rechtsgrundlage haben."*

15 Denjenigen, die personenbezogene Daten übertragen, wird folglich ein Ermessensspielraum eingeräumt, ob eine „gerechtfertigte Grundlage für die Annahme besteht, dass der Verkäufer über eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten verfügt". Im Umkehrschluss kann also die Einwilligungseinstellung einer betroffenen Person umgangen werden. Der Anbieter kann auf einer nicht näher spezifizierten „gerechtfertigten Grundlage" seinen Ermessensspielraum nutzen, um festzustellen, dass es einen rechtmäßigen Grund gibt, personenbezogene Daten an Dritte weiterzugeben, auch wenn eine Person die Zustimmung ausdrücklich verweigert hat. Das gesamte System stützt sich also auf das Ermessen und die Beurteilung des Anbieters auf Grundlage vager Begriffe mit unklar definierten Parametern und beruht nicht auf den Wünschen, der Kenntnisnahme oder der Zustimmung des Betroffenen.

16 Zusammenfassend lässt sich sagen, dass das Framework dem Verkäufer einen Ermessensspielraum einräumt, anstatt die Position des Betroffenen zu berücksichtigen. Dies steht im Widerspruch zu den gesetzlichen Anforderungen der DS-GVO. Das Framework versucht eine fiktive Zustimmung zu konstruieren, wobei sich die Verfasser darüber im Klaren sind, dass eine tatsächliche Zustimmung schwer zu erreichen ist. Angesichts der möglichen Verarbeitung von besonderen Kategorien personenbezogener Daten ist es durchaus verständlich, dass versucht wird, den Anbietern eine Form der Ermessensfreiheit einzuräumen. Bedauerlicherweise ist das Ergebnis nicht mehr als ein Feigenblatt hinsichtlich der Rechte der einzelnen Personen an ihren

Daten. Es gibt keine plausible Lesart des Frameworks, welche die individuellen Rechte angemessen berücksichtigt und schützt.

17 Wir stellen fest, dass IAB Europe kürzlich eine Presseerklärung veröffentlicht hat, in der eine Überarbeitung des Frameworks angekündigt wird. Diese Vorschläge werden aber nicht konkretisiert und die Ausführungen adressieren nicht die bestehenden Bedenken. Vielmehr weist die Presseerklärung darauf hin, dass es ein geeigneter Zeitpunkt für die Aufsichtsbehörden wäre, die gesamte Branche zu überprüfen, um eine konsistente und datenschutzkonforme Praxis zu erreichen.

ii. Authorized Buyers

18 Für Authorized Buyers gelten eine „Richtlinie" (guideline)[7] und Geschäftsbedingungen (terms of business). Die Richtlinie stößt auf eine Reihe von Bedenken.

19 Die Richtlinie verlagert die Verantwortung für den Datenschutz vom „Data Controller" auf Dritte, nämlich diejenigen, welche die Daten erhalten. So wird in der Richtlinie Folgendes ausgeführt:

RTB Callout Data Restriction

Zur Auswertung von Seitenaufrufen und von Angeboten auf Basis von Benutzerdaten, die [der Käufer] zuvor erhalten hat, kann [dieser] die verschlüsselte Cookie-ID und die mobile Werbekennung speichern. Alle anderen Callout-Daten mit Ausnahme von Positionsdaten können vom Käufer nach der Beantwortung eines Anzeigenaufrufs und nur zum Zweck der Vorhersage der Verfügbarkeit von Lagerbeständen durch das Authorized Buyers Program gespeichert werden. [Der] Käufer darf die Callout-Daten nur für die Dauer, die zur Erfüllung der oben genannten Zwecke erforderlich ist, und in keinem Fall länger als 18 Monate aufbewahren. Außer wenn [der] Käufer [die Auktion für] einen bestimmten Seitenaufruf gewinnt, ist folgendes nicht erlaubt: (i) Callout-Daten verwenden um mit diesem Seitenaufruf Benutzerlisten oder Benutzerprofile zu erstellen; (ii) Callout-Daten für diesen Seitenaufruf mit Daten Dritter verbinden; oder (iii) Rate Card Daten in irgendeiner Form, einschließlich aber nicht beschränkt auf Zusammenfassungen, mit Dritten teilen.

Datenschutz

Wenn [der] Käufer auf von Google zur Verfügung gestellte personenbezogene Daten, die eine Person direkt oder indirekt identifizieren und die ihren Ursprung im Europäischen Wirtschaftsraum haben („persönliche Daten"), zugreift, sie verwendet oder verarbeitet, gilt folgendes für [den] Käufer:

- *alle Datenschutz-, Datensicherheits- und Privatsphäregesetze, Richtlinien, Verordnungen und Regeln unter allen anwendbaren Gerichtsbarkeiten sind einzuhalten;*
- *Zugriff und Nutzung personenbezogener Daten ist nur für Zwecke gestattet, die mit der gegebenen Einwilligung der Person konform sind, deren personenbezogene Daten übermittelt wurden;*
- *Geeignete organisatorische und technische Maßnahmen zum Schutz der Mitarbeiter sind zu ergreifen, um die personenbezogenen Daten gegen Verlust, Missbrauch und unbefugten oder rechtswidrigen Zugriff, Offenlegung, Änderung und Vernichtung zu schützen; und*
- *es muss das gleiche Schutzniveau geboten werden, wie es die EU-US-Datenschutzrichtlinie (EU-US Privacy Shield Principles) vorschreibt.*

[Der] Käufer wird [die] Einhaltung dieser Verpflichtung regelmäßig überwachen und hat Google unverzüglich schriftlich zu benachrichtigen, wenn [der] Käufer nicht mehr in der Lage ist, dieser Verpflichtung nachzukommen (oder wenn es ein erhebliches Risiko gibt, dass [der] Käufer dieser Verpflichtung nicht mehr nachkommen kann) und in solchen Fällen wird [der] Käufer entweder die Verarbeitung personenbezogener Daten einstellen oder unverzüglich andere angemessene und geeignete Maßnahmen zur Behebung der Probleme, die einem angemessenen Schutzniveau im Wege stehen, ergreifen.

20 Der zitierte Abschnitt legt nahe, dass Authorized Buyer, sobald die personenbezogenen Daten an einen Käufer übermittelt werden, keine wirksame Kontrolle mehr darüber hat, wie diese Daten verwendet werden. Vielmehr wird akzeptiert, dass der Dritte (Käufer) befugt und in der Lage ist, diese Daten zu verwenden. Die einzigen Beschränkungen sind vertraglicher Natur und es ist unklar, inwieweit diese tatsächlich durchgesetzt werden oder werden könnten. Das Gleiche gilt für die „Google Ads Controller-Controller Data Protection Terms" von Google.[8]

21 Darüber hinaus werden sogar die auferlegten Einschränkungen ausgehöhlt. Zum Beispiel wird aus der Guideline nicht klar, welche Einschränkungen einem erfolgreichen Bieter auferlegt werden, denn die Einschränkungen gelten für erfolglose Bieter:

Außer wenn [der] Käufer [die Auktion für] einen bestimmten Seitenaufruf gewinnt, ist Folgendes nicht erlaubt: („Unless buyer wins a given impression, it must not ...").

Das offensichtliche Fehlen von Kontrolle gibt Anlass zu ernsthaften Bedenken hinsichtlich der technischen und organisatorischen Sicherheit der relevanten Daten.

22 Darüber hinaus hängt die Wirksamkeit der Datenschutzpolitik allein von den Dritten ab, die Authorized Buyer-Verletzungen freiwillig melden sollen. Es gibt keine ausreichenden technischen Maßnahmen zum Schutz personenbezogener Daten.

D. Die Probleme: Rechtliche Bedenken bezüglich Framework und Guidelines

23 Der oben dargestellte Hintergrund verdeutlicht, dass die Verarbeitung durch die Branche ein erhebliches Risiko für anhaltende Verstöße gegen das Datenschutzrecht und insbesondere gegen die DS-GVO birgt. Datenschutzaufsichtsbehörden berücksichtigen normative Rahmen wie Branchen-Frameworks, wenn es darum geht zu entscheiden, ob regulatorische Maßnahmen ergriffen werden

müssen.[9] Die Datenschutzbehörden werden daher ersucht, das IAB-Framework und Googles Guidelines bei der Prüfung der Notwendigkeit von Regulierungsmaßnahmen zu berücksichtigen.

24 Wir sind der Ansicht, dass eine Reihe der in Art. 5 DS-GVO genannten Datenschutzgrundsätze betroffen ist. In diesem Stadium und in Erwartung der Prüfung dieser Beschwerde werden unsere Bedenken hier nicht ausführlich dargelegt. Wir sind der Meinung, dass der Schwerpunkt in erster Linie auf der Prüfung der Rechtmäßigkeit der oben dargestellten Guidelines und Frameworks liegen sollte und nicht bei einzelnen Fällen und Verstößen. Wir fassen unsere wichtigsten Anliegen im Folgenden zusammen.

i. Integrität und Vertraulichkeit

25 Unsere Hauptsorge liegt darin, dass die derzeitigen Rahmenbedingungen und Regelungen der Branche keinen angemessenen Schutz gegen die unbefugte und potenziell unbegrenzte Weitergabe und Verarbeitung personenbezogener Daten bieten.

26 Gemäß Art. 5 Abs. 1 lit. f DS-GVO müssen die Daten „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)“.

27 Das Framework von IAB EUROPE und die Richtlinie von Google bieten insbesondere aus folgenden Gründen keine ausreichende „Integrität und Vertraulichkeit“ für personenbezogene Daten:

a Sie verlangen nicht, dass die betroffenen Personen über die Verbreitung ihrer Daten oder über die Absicht oder Entscheidung, ihre Daten an Empfänger weiterzugeben, informiert werden.

b Sie bieten Einzelpersonen keine Möglichkeit, sich bei Verkäufern / Empfängern von Daten dazu zu äußern, wie ihre personenbezogenen Daten verwendet werden dürfen.

c Sie verweigern den betroffenen Personen ein formelles Recht auf Widerspruch gegen die Verwendung ihrer Daten durch Dritte.

d Sie bieten keine oder keine ausreichende Kontrolle, um rechtswidrige und/oder genehmigte weitere Nutzungen zu kontrollieren.

ii. Rechtmäßigkeit und Fairness der Verarbeitung

28 Art. 5 Abs. 1 lit. a DS-GVO verlangt, dass personenbezogene Daten rechtmäßig und fair verarbeitet werden. Art. 6 DS-GVO beschreibt die Voraussetzungen einer rechtmäßigen Verarbeitung personenbezogener Daten. Nach Art. 6 Abs. 1 DS-GVO können nur zwei Rechtfertigungen für die Datenverarbeitung der Branche anwendbar sein:

i die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben (lit. a) oder

ii die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (lit. f).

29 Die Zustimmung bzw. Einwilligung ist die zentrale Voraussetzung für eine rechtmäßige Datenverarbeitung. Es liegt in der Natur der Branche, dass sie nicht in der Lage ist, eine angemessene Einwilligung einzuholen. Dies wird auch im Framework anerkannt. Dies gilt insbesondere für Vermittler, die möglicherweise keinen direkten Kontakt mit den Betroffenen haben.

30 Jeglicher Verweis auf berechtigte Interessen wäre bei breit gestreuten RTB-Gebotsanfragen fehl am Platz. Ein solches berechtigtes Interesse gilt nicht absolut, sondern muss mit den Interessen sowie Grundrechten und -freiheiten der Betroffenen abgewogen werden. Insbesondere wenn die personenbezogenen Daten an eine große Anzahl von Drittunternehmen weitergegeben werden, mit unbekannten Folgen und ohne angemessene Sicherheitsvorkehrungen, kann die Verarbeitung nicht als notwendig und/oder legitim gerechtfertigt werden, wenn man die möglichen Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen berücksichtigt.

31 Ferner bedarf gemäß Art. 9 Abs. 2 DS-GVO die Verarbeitung „besonderer Kategorien personenbezogener Daten“ der ausdrücklichen Einwilligung (lit. a), wenn diese Daten nicht durch den Betroffenen „offensichtlich öffentlich gemacht“ wurden (lit. e) und keine anderen Ausnahmen gelten. Dem gegenüber ermöglichen es das IAB-Framework und die Authorized Buyer-Richtlinie der Branche, Daten ohne Einwilligung zu verarbeiten, einschließlich direkter oder abgeleiteter Daten über die rassische/ethnische Herkunft, politische Meinungen, religiöse/philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben oder sexuelle Orientierung und zur eindeutigen Identifizierung verarbeitete biometrische sowie genetische Daten. Ohne ausdrückliche Einwilligung zu einer solchen Verarbeitung verstößt dieses Vorgehen gegen Art. 9 DS-GVO.

32 Darüber hinaus ist eine ausdrückliche Einwilligung erforderlich, wenn wesentliche, ausschließlich automatisierte Entscheidungen in Bezug auf eine Person getroffen werden. Die Artikel-29-Arbeitsgruppe legte fest, unter welchen Umständen davon ausgegangen werden muss, dass verhaltensorientierte Werbung, wie sie von der Branche durchgeführt wird, „erhebliche Beeinträchtigungen“ im Sinne von Art. 22 DS-GVO zur Folge hat.[10] Dies gilt insbesondere dann, wenn gefährdete Personen mit Dienstleistungen angesprochen werden, aus denen ihnen Nachteile erwachsen können, wie z. B. Glücksspiele oder bestimmte Finanzprodukte. Das Fehlen der Möglichkeit, die ausdrück-

liche Einwilligung einzuholen, ist eine Missachtung von Art. 22 DS-GVO.

33 Dementsprechend bestehen Bedenken, dass die Branche ohne wirksame Einwilligung persönliche Daten und speziell sensitive Daten verarbeitet. Das Framework sieht ein System vor, in dem Daten ohne Zustimmung der betroffenen Person verarbeitet und verbreitet werden dürfen. Dies ist nicht rechtmäßig. Eine solche Datenverarbeitung kann auf keinen Fall als „fair" oder „transparent" bezeichnet werden.

iii. Angemessenheit, Relevanz und Timing

34 Wir haben Bedenken, ob die Verarbeitung der Daten durch die Branche den Anforderungen aus Art. 5 Abs. 1 lit. c DS-GVO entspricht, der verlangt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt" verarbeitet werden. Die Anzahl der Empfänger der personenbezogenen Daten und die Möglichkeit, dass diese personenbezogenen Daten von den Empfängern weiterverwendet werden, kann schwerwiegende negative Konsequenzen nach sich ziehen.

35 Art. 5 Abs. 1 lit. e DS-GVO schreibt ferner vor, dass personenbezogene Daten, die für einen bestimmten Zweck oder bestimmte Zwecke verarbeitet werden, nicht länger aufbewahrt werden dürfen, als dies für diesen Zweck oder diese Zwecke erforderlich ist. Die Guidelines von Authorized Buyers sehen vor (auch wenn sie es aufgrund der fehlenden Kontrolle nicht garantieren können), dass personenbezogene Daten über einen längeren Zeitraum ohne identifizierbaren Zweck aufbewahrt werden.

iv. Data protection by design and default

36 Verhaltensbasierte Werbung hängt von der Fähigkeit ab, Menschen durch die Verwendung digitaler Identifikatoren, die an Geräte gebunden sind (die sich heute zumeist auf eine einzelne Person beziehen), auszusondern oder Verbindungen zu Personen über Geräte und Kontexte hinweg herzustellen. Zu diesen Identifikatoren gehören Web-Fingerabdrücke, die sich auf die eindeutige Einrichtung von Einzelgeräten und Cookies auf Geräten beziehen, so wie dies im Bericht von Dr. Ryan erläutert wird. Diese Identifikatoren sind für Einzelpersonen schwer nachvollziehbar oder abrufbar, um ihre Aufzeichnungen bei den Verantwortlichen, die ihre Informationen speichern, zu kontrollieren. Dies führt zu einem erheblichen Ungleichgewicht und stellt eine erhebliche Barriere für die betroffenen Personen dar, die es ihnen unmöglich macht, wichtige Datenschutzrechte durchzusetzen, wie z. B. die Rechte auf Auskunft, Löschung, Widerspruch, Einschränkung der Verarbeitung und Portabilität.

37 Dies wiederum unterstreicht ein breiteres Anliegen im Zusammenhang mit dem übergreifenden Grundsatz von Treu und Glauben in der DS-GVO (Art. 5 Abs. 1 lit. a): Die Verantwortlichen haben einfachen Zugang zu den Identifikatoren für einzelne Personen, während diese Personen selbst nicht wirklich in der Lage sind, die Identifikatoren zu verwenden oder zu kontrollieren. Dies führt insbesondere zu Bedenken im Hinblick auf Art. 25 DS-GVO, der den Verantwortlichen eine aktive Verpflichtung auferlegt, Datenschutzvorkehrungen wie z. B. für den Datenzugang oder für den Widerspruch in ihre Verfahren und Systeme aufzunehmen.

v. Datenschutz-Folgenabschätzung

38 Angesichts der Streuweite der personenbezogenen Daten und der besonders sensitiven Daten sowie der Vielzahl der Empfänger dieser Daten muss davon ausgegangen werden, dass die Verarbeitung zu einem „hohen Risiko für die Rechte und Freiheiten natürlicher Personen" führt. Dementsprechend verlangt Art. 35 DS-GVO jeweils eine angemessene Datenschutz-Folgenabschätzung. Nach unserem Kenntnisstand wurde bisher keine ordnungsgemäße Folgenabschätzung durchgeführt oder veröffentlicht.

E. Gerichtsbarkeit

39 Die Datenschutzaufsichtsbehörden sind für die Aktivitäten zuständig, die in dieser Stellungnahme angesprochen und im Ryan-Bericht beschrieben werden.

i. Verarbeitung personenbezogener Daten

40 Artikel 4 Nr. 1 DS-GVO definiert personenbezogene Daten als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person" beziehen. Dazu gehört auch „eine Online-Kennung", wenn sie es ermöglicht, eine Person direkt oder indirekt zu identifizieren. Der Europäische Gerichtshof (EuGH) hat bestätigt, dass IP-Adressen personenbezogene Daten darstellen können.[11] Darüber hinaus werden „pseudonymisierte" Daten zu einer Person weiterhin als personenbezogene Daten behandelt.

41 Die Verarbeitung und Verbreitung der personenbezogenen Daten einer betroffenen Person während des RTB-Prozesses umfasst auch die Verarbeitung von IP-Adressen oder detaillierterer personenbezogener Daten wie zum Beispiel Standortdaten.

ii. Gerichtsbarkeit

42 Die sich vorliegend beschwerenden Nichtregierungsorganisationen, die Digitale Gesellschaft, das Netzwerk Datenschutzexpertise, die Deutsche Vereinigung für Datenschutz sowie Digitalcourage haben ihren Sitz in der Bundesrepublik Deutschland und vertreten die Grundrechtsinteressen von Internet-Nutzenden in Deutschland.

43 Gemäß Art. 3 Abs. 2 lit. b DS-GVO gilt die Verordnung für Verantwortliche außerhalb der EU, wenn sich ihre Datenverarbeitung auf die Beobachtung des Verhaltens von Betroffenen in der EU bezieht.

44 Die Branche ist bestrebt, Werbeanzeigen für Kunden im jeweiligen Gebiet anzubieten; daher ist der Ort der Niederlassung der verschiedenen beteiligten Unternehmen für den Geltungsumfang der DS-GVO und die Zuständigkeit der deutschen Aufsichtsbehörden irrelevant.

45 Gemäß Art. 51 DS-GVO und § 40 BDSG sind die Datenschutzaufsichtsbehörden der Bundesländer die zuständige

Aufsichtsbehörden in Deutschland. Die Aufgaben der Aufsichtsbehörden sind in Art. 57 DS-GVO beschrieben und umfassen die Überwachung und Durchsetzung der DS-GVO. Um dieser Aufgabe gerecht zu werden, haben sie gemäß Art. 58 Abs. 1 lit. b DS-GVO die Befugnis, „Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen“.

46 Die Datenschutzaufsichtsbehörden sind mit der Bearbeitung von Beschwerden betraut, die von einer betroffenen Person gemäß Art. 77 DS-GVO eingereicht werden. Diese Beschwerde wird von den für die genannten Nichtregierungsorganisationen unterzeichnenden Personen auch im eigenen Namen eingereicht.

47 Eine entsprechende Beschwerde wurde beim irischen Datenschutzbeauftragten erhoben; weitere Beschwerden werden derzeit bei anderen nationalen Aufsichtsbehörden eingereicht. Angesichts der europaweiten Dimension der in dieser Beschwerde aufgeworfenen Fragen und Unternehmen erscheint es sinnvoll, dass die Aufsichtsbehörden dieses Thema gemeinsam prüfen. Wir fordern die deutschen Aufsichtsbehörden deshalb auf, mit anderen nationalen Aufsichtsbehörden zusammenzuarbeiten, um eine gemeinsame Untersuchung gemäß Art. 62 DS-GVO durchzuführen.

F. Anfragen

48 Die Datenschutzaufsichtsbehörden erhalten individuelle Beschwerden von Frau Elisabeth Niekrenz, Herrn Thilo Weichert, Herrn Frank Spaeing und Herrn Friedemann Ebelt. Alle vier genannten Unterzeichnenden nutzen das Internet und sind von der in dieser Beschwerde genannten verhaltensbasierten Werbung betroffen. Zusätzlich zur Prüfung der individuellen Beschwerde und deren Bescheidung bitten wir die Aufsichtsbehörden, im Rahmen ihrer Befugnisse und ihres Mandats weitere Schritte zu unternehmen.

49 Gemäß Art. 58 Abs. 1 lit b DS-GVO sind die Aufsichtsbehörden befugt, Datenschutzüberprüfungen durchzuführen. Die Verantwortlichen sind gemäß § 40 Abs. 4 BDSG verpflichtet, hierfür alle erforderlichen Auskünfte zu erteilen. Die Aufsichtsbehörden sind befugt, Einblick in relevante Dokumente zu nehmen und die stattfindende Datenverarbeitung zu überprüfen. Die Aufsichtsbehörden haben die Beschwerdeführer über die Ergebnisse der Überprüfung gemäß Art. 77 Abs. 2 DS-GVO zu unterrichten. Hierbei sollte auf folgende Umstände eingegangen werden:

a Es fehlen geeignete Garantien für Sicherheit und Integrität der genannten Daten.

b Personenbezogene Daten und besondere Kategorien personenbezogener Daten werden verarbeitet.

c Es ist fragwürdig, ob den Verarbeitungen wirksame Einwilligungen zugrunde liegen.

d Es fehlt an einer Datenschutz-Folgenabschätzung.

50 Wir fordern die Datenschutzaufsichtsbehörden auf, ihre Befugnisse sowohl gegenüber dem *IAB Europe Framework* als auch im Hinblick auf Googles *Authorized Buyers* auszuüben. Da es einzelnen Betroffenen, nicht zuletzt wegen des Umfangs und der Komplexität der genannten Geschäftspraktiken, nicht möglich ist zu bewerten, inwieweit die gesamte Branche die rechtlichen Verpflichtungen allgemein einhält, geschweige denn diese Einhaltung sicherzustellen, ist der Sachverhalt der verhaltensbasierten Werbung eine vorrangige Aufgabe für die Datenschutzaufsicht.

i. Verhaltenscodex (Code of practice)

51 Art. 40 DS-GVO sieht vor, dass Verbände und andere Vereinigungen Verhaltensregeln ausarbeiten können, die präzisierend eine „faire und transparente Verarbeitung“ mit einer Vielzahl von Vorkehrungen regeln. Diese sollen von den Aufsichtsbehörden gefördert werden und sind letztlich von diesen zu genehmigen. Es ist wünschenswert, dass für personalisierte Werbung derartige mit den Anforderungen der DS-GVO konforme Verhaltensregeln ausgearbeitet und dass deren Einhaltung im Rahmen regulierter Selbstregulierung überwacht wird.

52 Es steht außer Frage, dass die öffentlich dokumentierten Aktivitäten der Branche, wie sie im Bericht von Dr. Ryan dargelegt werden, Leitlinien (good practice guidance) für diese Branche notwendig machen, um sicherzustellen, dass das Datenschutzrecht eingehalten wird und dass so die Rechte der Betroffenen gewahrt bleiben. Einzelfallklagen von Betroffenen werden nicht ausreichen, um den weitreichenden Bedenken hinsichtlich der Praktiken der Branche im Sinne des öffentlichen Interesses Rechnung zu tragen. Die Datenschutzaufsichtsbehörden werden dringend aufgefordert, Maßnahmen zu ergreifen und Leitlinien speziell für diesen Teil des Profiling-Sektors zu erstellen.

ii. Einvernehmliche Prüfung (Consensual audit)

53 Den Aufsichtsbehörden ist es erlaubt, einvernehmliche Prüfungen durchzuführen. Angesichts der weitreichenden und systematischen Probleme, die in der vorliegenden Beschwerde sowie in dem Bericht von Dr. Ryan aufgezeigt wurden, ersuchen wir die Aufsichtsbehörden, im Rahmen ihrer Befugnisse einvernehmliche Prüfungen bei den beteiligten Unternehmen anzustreben, um in der gesamten Branche eine gute Praxis durchzusetzen. Werden die Untersuchungs- und Abhilfebefugnisse der Datenschutzaufsicht nicht umfassend wahrgenommen, so erscheint es unwahrscheinlich, dass die tief verwurzelten und sich weiter verschlimmernden Probleme gelöst werden können. Parallel zu den vorliegenden Beschwerden werden *IAB Europe* und *Google Authorized Buyers* angeschrieben und dabei aufgefordert, einer solchen Untersuchung freiwillig zuzustimmen und diese aktiv zu unterstützen.

G. Nächste Schritte

54 Aus den oben genannten Gründen werden die Datenschutzaufsichtsbehörden gebeten, eine allgemeine Untersuchung der Tätigkeiten der Branche einzuleiten und die in dieser Vorlage beschriebenen Maßnahmen zu ergreifen.

55 Eines der großen Probleme bei den oben beschriebenen Formen der Datenverarbeitung ist, dass sie so umfangreich und komplex sind, dass sie jede und jeden zu jeder Zeit betreffen können. Es betrifft Individuen, einschließlich schutzbedürftiger Personen, in allen Lebensbereichen und in der gesamten Europäischen Union. Wir fordern die deutschen Datenschutzaufsichtsbehörden daher auf, mit den Kollegen in den anderen Mitgliedstaaten zusammenzuarbeiten, um eine gemeinsame Untersuchung gemäß Art. 62 DS-GVO durchzuführen. Wir behalten uns das Recht vor, diese Beschwerde gegebenenfalls durch weitere Beweise und Argumente zu ergänzen. In der Zwischenzeit zögern Sie bitte nicht, uns zu kontaktieren, wenn wir Ihnen weiterhelfen können. Wir wären Ihnen dankbar, wenn Sie uns gemäß Art. 77 Abs. 2 DS-GVO über die als Reaktion auf diese Beschwerde ergriffenen Maßnahmen auf dem Laufenden halten würden.

Elisabeth Niekrenz, Digitale Gesellschaft, Groninger Straße 7, 13347 Berlin

Thilo Weichert, Netzwerk Datenschutzexpertise, Waisenhofstr. 41, 24103 Kiel

Frank Spaeing, Deutsche Vereinigung für Datenschutz, Reuterstraße 157, 53113 Bonn

Friedemann Ebelt, Digitalcourage, Marktstraße 18, 33602 Bielefeld

Berlin, Kiel, Bonn, Bielefeld,
4. Juni 2019

1 https://brave.com/Behavioural-advertising-and-personal-data.pdf; s. S. 133.

2 Siehe Leitlinien für automatisierte individuelle Entscheidungsfindung und Profilerstellung im Sinne der Verordnung 2016/679 (wp251rev.01, S. 16): „Durch Profiling können Daten besonderer Kategorien erzeugt werden, indem aus Daten, die an sich keine besondere Datenkategorie bilden, dies aber in Kombination mit anderen Daten tun, Daten abgeleitet werden. So kann beispielsweise aus den Lebensmitteleinkäufen einer Person, die mit Daten zur Qualität und zum Energiegehalt von Lebensmitteln verknüpft werden, der Gesundheitszustand der betroffenen Person hergeleitet werden.“ Es sei auch darauf hingewiesen (wie vom CJEU in Nowak bestätigt wird), dass Daten, wie z. B. Schlussfolgerungen, die sich auf eine Person beziehen, aber unrichtig sind, personenbezogene Daten bleiben. Wäre dies nicht der Fall, könnte das „Recht auf Richtigstellung“ niemals eingefordert werden.

3 Dieses Problem wird verschärft durch die Tatsache, dass die Unternehmen weitgehend unbekannt und für die betroffene Person unzugänglich sind, da die für die Datenerfassung Verantwortlichen (Controller), welche die Daten zunächst sammeln, selten explizite Informationen über die Empfänger oder auch nur über Kategorien von Empfängern liefern, und die Empfänger die betroffenen Personen nicht gemäß ihren Verpflichtungen nach Art. 14 DS-GVO über den Erhalt dieser Daten informieren.

4 https://iabeurope.eu/tcfdocuments/documents/legal/currenttcftncFINAL.pdf.

5 Zitat aus dem Framework (Betonung nicht im Originaldokument): „Wenn ein CMP der festen Überzeugung ist, dass ein Verkäufer nicht mit der Spezifikation, den Richtlinien oder dem Gesetz übereinstimmt, muss er unverzüglich einen Bericht mit dem MO gemäß den MO-Verfahren einreichen und **kann**, wie in den MO-Verfahren vorgesehen, die Zusammenarbeit mit einem Verkäufer unterbrechen, solange die Angelegenheit untersucht wird“. Dies eröffnet dem für die Verarbeitung Verantwortlichen (Controller) einen vollständigen Ermessensspielraum bei der weiteren Verarbeitung und Verbreitung personenbezogener Daten, auch wenn diesem Controller bekannt ist, dass der Empfänger gegen die Datenschutzbestimmungen verstößt.

6 Im Ryan-Bericht (S. 5) wird dargestellt, dass die heute berüchtigte Firma Cambridge Analytica nur ein Beispiel für die Art der Endempfänger solcher Daten war.

7 https://www.google.com/doubleclick/adxbuyer/guidelines.html.

8 https://privacy.google.com/businesses/controllerterms/.

9 Für Großbritannien https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/.

10 Working Paper 251rev.01 (Fußnote 1) S. 10: „In vielen typischen Fällen wird die Entscheidung, auf Profiling beruhende gezielte Werbung zu präsentieren, Personen nicht in ähnlicher Weise erheblich beeinträchtigen, zum Beispiel wenn Werbung für einen Online-Shop eines Mainstream-Modehändlers angezeigt wird, die auf folgendem einfachen demografischen Profil beruht: „Frauen im Raum Brüssel im Alter von 25 bis 35 Jahren, die wahrscheinlich Interesse an Mode und bestimmten Bekleidungsartikeln haben“.

Es ist allerdings möglich, dass es in Abhängigkeit von den jeweiligen Umständen doch zu erheblichen Beeinträchtigungen kommt, beispielsweise

- durch den eingreifenden Charakter des Profiling-Prozesses, wenn beispielsweise Personen über mehrere Websites, Geräte oder Dienste verfolgt werden;
- die Erwartungen und Wünsche der betroffenen Personen;
- die Art und Weise der Werbeanzeige oder
- die Ausnutzung von Schwachstellen der betroffenen Personen, an die sich die Anzeige richtet.“

11 EuGH 19.10.2016 – C-582/14 (Breyer).

Bericht von Dr. Johnny Ryan

Verhaltensbasierte Werbung und persönliche Daten

Übersetzung ins Deutsche: Elisabeth Niekrenz

1. Hintergrund und Expertise

Mein Name ist Johnny Ryan. Ich bin leitender politischer Referent bei Brave, einem auf Datenschutz spezialisierten Internetbrowser.

Ich bin sowohl in der Ad-Tech-Branche als auch im Verlagswesen tätig gewesen. Bevor ich zu Brave kam, war ich bei PageFair, einem Werbetechnologieunternehmen, beschäftigt. In dieser Funktion war ich in Arbeitsgruppen tätig, die Standards für die Werbebranche entwickelten. Davor arbeitete ich als Chief Innovation Officer bei der Zeitung Irish Times.

Zudem war ich in Wissenschaft und Politik tätig und bin Autor zweier Bücher: Bei dem ersten handelt es sich um eine Geschichte der Technologie, die bereits auf Lektürelisten in Harvard und Stanford stand. Das andere diente der Europäischen Kommission als am häufigsten zitierte Quelle in ihrer Folgenabschätzung, die sich gegen eine Web-Zensur in der gesamten Europäischen Union entschied. Ich bin Fellow der Royal Historical Society und Mitglied des Expertennetzwerks des Weltwirtschaftsforums für Medien, Unterhaltung und Information.

Ich habe an der University of Cambridge mit einer Arbeit promoviert, die die Verbreitung von militanten Memes im Netz untersuchte.

Meine Analysen über die Online-Medien- und Werbebranche sind in Medien wie The New York Times, The Economist, The Financial Times, Wired, Le Monde, NPR, Advertising Age, Fortune, Business Week, BBC, Sky News und vielen anderen erschienen.

2. Wie personenbezogene Daten für verhaltensbasierte Online-Werbung verwendet werden

Jedes Mal, wenn eine verhaltensorientierte Werbeanzeige an eine Person gerichtet wird, die eine Website besucht, sendet das System, das die Werbeanzeige auswählt,[1] persönliche Daten an Hunderte oder Tausende von Unternehmen.

Zu diesen personenbezogenen Daten gehören die URL jeder Seite, die ein Benutzer besucht, seine IP-Adresse (aus der sich die geografische Position ableiten lässt), Details zu seinem Gerät und verschiedene eindeutige IDs, die zuvor über den Benutzer gespeichert wurden, um ein langfristiges Profil über ihn oder sie aufzubauen.

Bei diesem System handelt es sich um eine relativ junge Entwicklung der Online-Medien. Erst im Dezember 2010 hat sich ein Konsortium[2] von Unternehmen der Werbetechnik (im Folgenden AdTech) auf die Methoden von Tracking und Werbung geeinigt. Zuvor wurde Online-Werbung durch weitaus einfachere Netzwerke, die Werbeplätze auf Websites verkauften, oder durch sehr lukrative Direktverkaufsgeschäfte von Verlagen platziert.[3]

Wie im Folgenden ausgeführt, hat die Ad-Tech-Industrie trotz der Übergangsfrist bis zum Inkrafttreten der Datenschutz-Grundverordnung keine angemessenen Maßnahmen ergriffen, um geltendes Datenschutzrecht bei der Vielzahl von Unternehmen, die Daten erhalten, durchzusetzen.

3. Wie personenbezogene Daten verbreitet werden

Ein großer Teil der Online-Medien- und Werbebranche verwendet ein System namens „RTB“, was für „Real Time Bidding“ steht. Es gibt zwei Versionen:

- „OpenRTB“ wird von den bedeutendsten Unternehmen der Online-Medien- und Werbebranche eingesetzt.
- „Authorized Buyers“, Googles proprietäres RTB-System, das kürzlich von „DoubleClick Ad Exchange“ (bekannt als „AdX“) in „Authorized Buyers“ umbenannt wurde.[4]

Google verwendet sowohl OpenRTB als auch Authorized Buyers.[5]

Die Fachspezifikationen von OpenRTB sind über das in New York ansässige IAB TechLab öffentlich zugänglich.[6] Die Fachspezifikationen von Authorized Buyers werden von Google öffentlich zur Verfügung gestellt.

Diese Dokumente zeigen, dass jedes Mal, wenn eine Person eine Seite auf einer Website lädt, die Real Time Bidding verwendet, persönliche Daten über sie an Dutzende – oder Hunderte – von Unternehmen übertragen werden. Beispielsweise können folgende personenbezogene Daten übermittelt werden:

- Welche Website die Nutzerin oder der Nutzer besucht
- Der Standort (OpenRTB enthält auch die vollständige IP-Adresse)
- Eine Beschreibung des verwendeten Geräts
- Eindeutige Tracking-IDs oder ein „Cookie-Match“, mit denen Werbetreibende versuchen können den Nutzer oder die Nutzerin bei ihrem nächsten Besuch zu identifizieren, damit ein langfristiges Profil mit Offline-Daten aufgebaut oder gefestigt werden kann
- IP-Adresse (je nach Version des Systems RTB)
- Segment-ID des Datenvermittlers, falls vorhanden. Dies kann Dinge wie die Einkommensklasse, Alter und Geschlecht, Gewohnheiten, Social-Media-Einfluss, Ethnie, sexuelle Orientierung, Religion und politische Orientierung der Nutzerin oder des Nutzers umfassen (je nach Version des Systems RTB)

Eine vollständige Zusammenfassung der personenbezogenen Daten in Open RTB-Anfragen, die von allen RTB-Werbeunternehmen, einschließlich Google, genutzt werden, findet sich in Anhang 1*.

Eine Zusammenfassung der personenbezogenen Daten in den Authorized-Buyers-Anfragen finden Sie unter Anhang 2*.

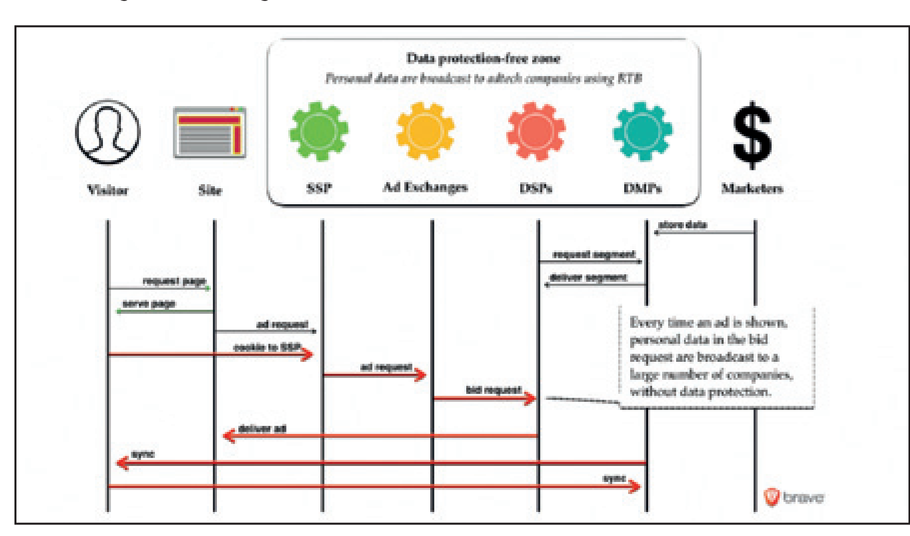
Relevante Auszüge aus den OpenRTB „AdCOM“-Fachspezifikationen sind in Anhang 3* dargestellt, Auszüge aus Googles proprietärer RTB-Spezifikation in Anhang 4*.

Zur Arbeitsweise

Die Übermittlung von personenbezogenen Daten findet bei der Gebotsanfrage („RTB bid request“) statt. Diese Gebotsanfrage wird in der Regel weit verbreitet, da das Ziel darin besteht, Angebote von Unternehmen einzuholen, die eine Anzeige an die Person senden möchten, die gerade die Website geladen hat. Eine RTB-Gebotsanfrage wird durch Unternehmen, die als „Supply Side Platforms“ (SSPs) bezeichnet werden, im Auftrag der Website verbreitet.

Das folgende Diagramm zeigt, wie personenbezogene Daten im Rahmen von Ausschreibungen an mehrere Demand Side Partner (DSP) übertragen werden, die dann entscheiden, ob sie Angebote abgeben. Der DSP handelt im Auftrag von Werbetreibenden und entscheidet auf Basis des Personenprofils, auf das der Werbetreibende abzielt, wann ein Angebot abgegeben wird.

Teilweise benutzen Data Management Plattformen, zu denen Cambridge Analytica gehört, die Daten, die sie so erhalten, um ihre bereits existierenden Personenprofile zu erweitern. Diese Synchronisierung wäre ohne die Gebotsanfragen nicht möglich.



Der wirtschaftliche Anreiz für viele Ad-Tech-Unternehmen besteht darin, so viele Daten wie möglich mit so vielen Partnern wie möglich zu teilen und sie an Partnerunternehmen, die Datenvermittlungen betreiben, weiterzugeben. Offenkundig ist die Weitergabe personenbezogener Daten an ein solches Umfeld hoch riskant.

Trotz dieses hohen Risikos hat RTB keine Mechanismen eingerichtet, die kontrollieren, was mit diesen personenbezogenen Daten passiert, sobald ein SSP oder eine Anzeigenbörse eine Gebotsanfrage sendet. Auch wenn der Anfrageverkehr sicher ist, gibt es keine technischen Maßnahmen, die den Empfänger einer Gebotsanfrage daran hindern, die Daten zu verkaufen oder durch Kombination mit anderen Daten ein Profil zu erstellen. Mit anderen Worten: Es gibt keinen Datenschutz.

Das „GDPR Transparency & Consent Framework“ des IAB Europe besagt, dass ein Unternehmen, das personenbezogene Daten erhält, diese nur mit anderen Unternehmen teilen sollte, wenn „eine gerechtfertigte Annahme dafür besteht, dass der Empfänger über eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten verfügt.[7] Mit anderen Worten: Die Branche verfolgt einen „trust everyone“-Ansatz zum Schutz der sehr intimen Daten, sobald sie einmal übertragen wurden.

Es gibt keine technischen Maßnahmen, um die Daten angemessen zu schützen. Das IAB Europe hat kürzlich angekündigt, dass es in Zusammenarbeit mit einer Organisation namens Media Trust ein Tool entwickelt, mit dem versucht werden soll, festzustellen, ob die „consent management platforms“ (CMPs), die am IAB Europe teilnehmen, den Richtlinien des Frameworks entsprechen. Laut einer Pressemitteilung von IAB validiert das Tool, ob der Code eines CMPs mit den Anforderungen der technischen Spezifikationen und Protokolle, die im IAB Europe Transparency & Consent Framework detailliert beschrieben sind, entspricht.[8]

Dieses Tool, das sich derzeit in der Beta-Phase befindet, wird nicht ausreichen, um persönliche Daten zu schützen, die in Gebotsanfragen übertragen werden. Denn - auch wenn es möglich wäre, alle webbasierten Datenübertragungen zu kontrollieren[9] - gäbe es immer noch keine Möglichkeit herauszufinden, ob ein Unternehmen z. B. einen kontinuierlichen Server-zu-Server-Transfer von personenbezogenen Daten an andere Unternehmen eingerichtet hat.

Sobald die personenbezogenen Daten in einer Ausschreibung an eine große Anzahl von Unternehmen weitergegeben werden, ist das Spiel vorbei. Mit anderen Worten, sobald DSPs personenbezogene Daten erhalten, können sie nach Belieben mit diesen personenbezogenen Daten mit Geschäftspartnern handeln.

Dies ist besonders gravierend, da es sich häufig um Daten besonderer Kategorien handelt. Die betreffenden personenbezogenen Daten zeigen, was eine Person online tut, und geben oftmals einen bestimmten Standort preis. Dies allein kann Aufschluss über die sexuelle Orientierung der Person, den Glauben, die politische Orientierung oder die ethnische Zugehörigkeit geben. Zusätzlich gibt eine Segment-ID an, in welche Personenkategorie ein Data Broker oder ein langfristiger Profiler eine Person einordnet.

Darüber hinaus ist sich die Branche der Mängel dieses Ansatzes bewusst, verfolgt ihn aber dennoch weiter.

RTB-Gebotsanfragen müssen nicht unbedingt personenbezogene Daten enthalten. Wenn alle Akteure der Branche sich damit einverstanden erklären und die Normen unter der Leitung des IAB verändert würden, könnten nur Anfragen, die keine personenbezogenen Daten enthalten, zwischen Unternehmen weitergeleitet werden, sodass die Relevanz einer Werbeanzeige an dem Kontext der Website ausgerichtet würde. Dies würde die beteiligten Unternehmen an der Erstellung von Perso-

nenprofilen hindern, was sich auf ihre Einnahmen auswirken würde. Die Industrie ist gerade dabei, eine neue RTB-Spezifikation zu entwickeln (OpenRTB 3.0), die weiterhin personenbezogene Daten sendet, ohne dass Schutzvorkehrungen bestünden. In Anhang 4* wird OpenRTB 3.0 genauer dargestellt.

Online-Werbung, die diesen Ansatz nutzt, wird weiterhin Details darüber, was Personen im Internet lesen oder ansehen, an eine große Anzahl von Unternehmen verbreiten. Die personenbezogenen Daten sind nicht geschützt. Die Verbreitung erfolgt dauernd, sie geschieht auf praktisch jeder Website, jedes einzelne Mal, wenn eine Person eine Seite aufruft.

Dies ist eine weit verbreitete beunruhigende Praxis. Aufgrund des Umfangs der Branche sind die Grundrechte praktisch jeder Person, die in Europa das Internet nutzt, beeinträchtigt.

4. Bedenken gegenüber diesen Praktiken (Mediale Berichterstattung, Untersuchung von Nichtregierungsorganisationen, aufsichtsbehördliche Betrachtung usw.)

Mehrjährige Erhebungsdaten zeigen, dass in der Gesellschaft grundlegende und weitverbreitete Bedenken gegenüber diesen Praktiken herrschen. Eine Umfrage des britischen Information Commissioners, veröffentlicht im August 2018, berichtet, dass 53% der britischen Erwachsenen besorgt sind, über „Online-Aktivitäten verfolgt zu werden“.[10]

Im Jahr 2017 wurde die GFK vom IAB Europe beauftragt, 11.000 Menschen in der gesamten EU über ihre Einstellung zu Online-Medien und Werbung zu befragen. Die GFK berichtete, dass es nur „20 % gut finden würden, wenn ihre Daten zu Werbezwecken an Dritte weitergegeben werden“.[11] Dies steht in engem Zusammenhang mit der Umfrage, die die GFK 2014 in den Vereinigten Staaten durchführte und die ergab, dass „7 von 10 Baby Boomers (geboren nach 1969) und 8 von 10 Pre-Boomers (geboren vor 1969) Misstrauen gegenüber dem Umgang von Werbetreibenden mit ihren Daten haben“.[12]

Im Jahr 2016 ergab eine Eurobarometer-Umfrage unter 26.526 Personen in der Europäischen Union Folgendes:

„Sechs von zehn (60%) Befragten haben bereits die Datenschutzeinstellungen für ihren Internetbrowser geändert und vier von zehn (40%) vermeiden bestimmte Websites, weil sie besorgt sind, dass ihre Online-Aktivitäten überwacht werden. Über ein Drittel (37%) verwendet Software, die sie davor schützt, Online-Werbung angezeigt zu bekommen und mehr als ein Viertel (27%) nutzt Software, die verhindert, dass ihre Online-Aktivitäten überwacht werden“.[13]

Dies entspricht einer früheren Eurobarometer-Umfrage ähnlichen Umfangs aus dem Jahr 2011, in der festgestellt wurde, dass „70% der Europäer besorgt sind, dass ihre personenbezogenen Daten bei Unternehmen für einen anderen Zweck als den, für den sie gesammelt wurden, verwendet werden“.[14]

Die gleichen Bedenken bestehen auch in den Vereinigten Staaten. Im Mai 2015 hat das Forschungszentrum Pew Research Centre berichtet:

„76% der Erwachsenen in den Vereinigten Staaten sagen, dass sie ‚weniger Vertrauen haben‘ oder ‚überhaupt kein Vertrauen haben‘, dass die Aufzeichnungen über ihre Aktivitäten durch Online-Werbetreibende privat und sicher bleiben.“[15]

Tatsächlich hatten die Befragten am wenigsten Vertrauen, dass die Online-Werbebranche die personenbezogenen Daten über sie vertraulich und sicher verarbeitet verglichen mit jeder anderen Kategorie von Datenverarbeitern, einschließlich Social Media Plattformen, Suchmaschinen und Kreditkartenunternehmen. 50% sagte, dass keine Informationen an „Online-Werber“ weitergegeben werden sollten.[16]

In einer Reihe von Umfragen äußern große Mehrheiten ihre Besorgnis über AdTech. Die britische Royal Statistical Society veröffentlichte Forschungsergebnisse über das Vertrauen in Daten und die Einstellung zu Datennutzung und Datenaustausch im Jahr 2014 und stellte fest:

„Die Öffentlichkeit zeigte nur sehr wenig Unterstützung für Online-Händler, die zuletzt angesehene Seiten beobachten und zielgerichtete Anzeigen senden; 71% der Befragten meinten, dass dies nicht geschehen sollte“.[17]

Ähnliche Ergebnisse sind in der eigenen Forschung der Marketingbranche zu verzeichnen. RazorFish, eine Werbeagentur, führte eine Studie mit 1.500 Personen in Großbritannien, den USA, China und Brasilien im Jahr 2014 durch, die ergab, dass 77% der Befragten Werbung, mit der sie auf dem Handy angesprochen werden, als einen Angriff auf ihre Privatsphäre ansehen.[18]

Diese Bedenken manifestieren sich in der Art und Weise, wie sich Menschen heute online verhalten. Das enorme Wachstum von Adblocking-Tools (auf 615 Millionen aktiven Geräten bis Anfang 2017)[19] über den gesamten Zeitraum hinweg zeigt die globale Sorge von Internetnutzenden, von der Werbebranche verfolgt zu werden. Ein Branchenkommentator nannte dies den „größten Boykott der Geschichte“.[20]

Die Sorge um den Missbrauch personenbezogener Daten in der verhaltensorientierten Online-Werbung wird der Öffentlichkeit nicht kommuniziert. Selbst renommierte Werbetreibende, die Kampagnen online bezahlen, teilen die Sorge. Im Januar 2018 schrieb der CEO des Weltverbandes der Werbetreibenden, Stephan Loerke, einen Kommentar in AdAge, der die aktuellen Systeme als „Data free-for-all“ („Datenzugriff für alle“), attackierte, wobei „jede gezeigte Anzeige Daten beinhaltet, die von bis zu fünfzig Unternehmen berührt wurde, so die Programmexperten Labmatik“.[21]

5. Kommunikation mit den betroffenen Unternehmen

Am 16. Januar 2018 habe ich an den Vertreter der Arbeitsgruppe IAB Europe geschrieben (via IAB UK), um privat Feedback zu einem nicht-öffentlichen Entwurf der vom IAB geführten Industrie zur Reaktion auf die DSGVO zu geben. Ich habe Folgendes hervorgehoben.

Erstens würden Angebotsanfragen personenbezogener Daten zu vielen Parteien gelangen, ohne dass irgendein Schutz bestünde. Dies würde gegen Artikel 5 DSGVO verstoßen.

Zweitens mangele es aufgrund der Zusammenführung einer Vielzahl von Zwecken und inadäquater Information an einer informierten Einwilligung, was die Einwilligung unwirksam mache.

Obwohl mir für meinen Beitrag gedankt wurde, erhielt ich keine substanziierte Antwort.

Am 21. Februar 2018 habe ich in einem Videoanruf mit dem Koordinator

der IAB TechLab-Arbeitsgruppe, die verantwortlich für die Entwicklung der neuen OpenRTB-Fachspezifikation ist, meine Besorgnis über die Verbreitung von persönlichen Daten zum Ausdruck gebracht.

Aber als das IAB im März sein DS-GVO-Framework veröffentlichte, erfuhr ich, dass keine dieser Bedenken berücksichtigt wurde. Am 20. März 2018 habe ich meine Original-Einschätzung in einem offenen Brief veröffentlicht.

Dieser ist online unter https://pagefair.com/blog/2018/iab-europe-consent-problems/ zu finden.

Am 4. September 2018 habe ich im Namen von Brave einen ausführlichen Brief an das IAB und an das IAB TechLab geschrieben, um problematische Datenschutzfehler in OpenRTB 3 aufzuzeigen. Ich habe im Detail die akute Gefahr der Übermittlung der personenbezogenen Daten eines Website-Besuchers in Angebotsanfragen dargelegt. Der Brief ist verfügbar unter
https://brave.com/wp-content/uploads/2018/09/feedback-on-the-beta-OpenRTB-3.0-specification-.pdf.

Am 5. September 2018 antwortete das IAB mit einer vierzeiligen E-Mail, die den Antrag ablehnte.

1 Dieses System wird auch als Real Time Bidding bezeichnet.

2 Das Konsortium bestand aus DataXu, MediaMath, Turn, Admeld, PubMatic und The Rubicon Project. Siehe einen Hinweis zur Geschichte von OpenRTB in „OpenRTB API Specification Version 2.4, final draft“, IAB Tech Lab, März 2016 (URL: https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-4-FINAL.pdf), S. 2-3.

3 Erst 2006 entstand die erste „Anzeigenbörse“, die es den Werbenetzwerken ermöglicht, auf den Websites ihrer Kunden Flächen an potenzielle Käufer zu versteigern. Ein Pionier war Right Media, das von Yahoo! gekauft wurde. „RMX Direct: alternative ad networks battle for your blog“, Tech Crunch, 12. August 2006 (URL: https://techcrunch.com/2006/08/12/rmx-direct-alternative-ad-networks-battle-for-your-blog/?_ga=2.239524803.1716001118.15363).

4 „Introducing Authorized Buyers“, Authorized Buyers, Google (URL: https://support.google.com/adxbuyer/answer/9070822 , abgerufen am 24. August 2018).

5 „OpenRTB Integration“, Authorized Buyers, Google (URL: https://developers.google.com/authorized-buyers/rtb/openrtb-guide , abgerufen am 24. August 2018).

6 Das IAB (Interactive Advertising Bureau) ist die Standardisierungsorganisation und Interessenvertretung der globalen Werbetechnikbranche. Alle bedeutenden Ad-Tech-Unternehmen sind Mitglieder. Das IAB verfügt über lokale Franchiseunternehmen auf der ganzen Welt. Die Organisation, die Standards setzt, ist das IAB TechLab.

7 „IAB Europe Transparency & Consent Framework - Policies“, IAB Europe, 25. April 2018 (URL: https://iabeurope.eu/tcfdocuments/documents/legal/currenttcftncFINAL.pdf), S. 7.

8 „IAB Europe Press Release: IAB Europe CMP Validator Helps CMPs Align with Transparency & Consent Framework“, IAB Europa, 12. September 2018 (URL: https://www.iabeurope.eu/all-news/press-releases/iab-europe-press-release-iab-europe-cmp-validator-helps-cmps-align-with-transparency-consent-framework/).

9 Siehe „Data Compliance“, The Media Trust Website (URL: https://mediatrust.com/how-we-help/data-compliance).

10 „Information rights strategic plan: trust and confidence“, Harris Interactive for the Information Commissioner's Office, August 2018, S. 21.

11 „Europe online: an experience driven by advertising. Summary results“, IAB Europe, September 2017 (URL: http://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf), S. 7.

12 „GFK survey on data privacy and trust: data highlights“, GFK, Juli 2015, S. 29.

13 „Eurobarometer: E-Privacy (Eurobarometer 443)“, Europäische Kommission, Dezember 2016 (URL: http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124), S. 5, 36-7.

14 „Special Eurobarometer 359: attitudes on data protection and electronic identity in the European Union“, Europäische Kommission, Juni 2011, S. 2.

15 Mary Madden und Lee Rainie, „Americans' view about data collection and security“, Pew Research Center, Mai 2015 (URL: http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf), S. 7.

16 Mary Madden und Lee Rainie, „Americans' view about data collection and security“, Pew Research Center, May 2015 (URL: http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf), S. 25.

17 „The data trust deficit: trust in data and attitudes toward data use and data sharing“, Royal Statistical Society, Juli 2014, S. 5.

18 Stephen Lepitak, „Three quarters of mobile users see targeted adverts as invasion of privacy, says Razorfish global research“, The Drum, 30. Juni 2014 (URL: https://legacy.thedrum.com/news/2014/06/30/three-quarters-mobile-users-see-targeted-adverts-invasion-privacy-says-razorfish).

19 „The state of the blocked web: 2017 global adblock report“, PageFair, Januar 2017 (https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf).

20 Doc Searls, „Beyond ad blocking - the biggest boycott in human history“, Doc Searls Weblog, 28 September 2015 (https://blogs.harvard.edu/doc/2015/09/28/beyond-ad-blocking-the-biggest-boycott-in-human-history/).

21 Stephan Loerke, „GDPR data-privacy rules signal a welcome revolution“, AdAge, 25. Januar 2018 (URL: http://adage.com/article/cmo-strategy/gdpr-signals-a-revolution/312074/).

* Die Anhänge finden Sie im „Report from Dr. Johnny Ryan – Behavioural advertising and personal data“ unter https://brave.com/Behavioural-advertising-and-personal-data.pdf

Friedemann Ebelt

Online-Werbung reparieren – für Journalismus und Grundrechte

Digitalcourage hat die Beschwerde gegen invasives Real Time Bidding mit eingereicht, um auf das zu Grunde liegende Geschäftsmodell aufmerksam zu machen. Privatsphäre und Grundrechte sind keine Waren – darum muss die Online-Werbebranche repariert werden.

Wie das Geschäft mit der Versteigerung von Werbung im Internet technisch organisiert ist und an welchen Stellen es mit geltendem Datenschutzrecht kollidiert, hat Dr. Thilo Weichert in seinem Beitrag zu dieser Ausgabe der DANA dargelegt.

Digitalcourage unterstützt die von Johnny Ryan initiierte Beschwerde aber auch, um deutlich zu machen, dass kommerzielles Tracking im Internet kein exklusives Anliegen von Datenschützer.innen, Jurist.innen und Techniker.innen ist. Denn nahezu alle Menschen im Internet sind betroffen – aber kaum jemand ist informiert. Die Folge ist ein Ungleichgewicht der Macht zwischen der AdTech-Industrie und ihren Datenquellen, die ablenkend Kundschaft oder etwas treffender Zielgruppe genannt werden. Es ist höchste Zeit, dass die von der Werbeindustrie observierten Zielgruppen aus ihrer Passivität heraustreten und bei der Gestaltung des Internets mitmischen.

Zu diesem Zweck koordiniert die Civil Liberties Union for Europe die Kampagne #StopSpyingOnUs. Mit dieser Kampagne können alle Menschen sich über die Datenweitergabe bei Real Time Bidding informieren und erfahren, wie sie die Beschwerde auch im eigenen Namen bei ihren zuständigen Datenschutzbehörden einreichen können.[1]

Real Time Bidding ist Marketing-Sprech

In der Werbeindustrie bezeichnet der Begriff Real Time Bidding ein Geschäftsmodell, das helfen soll, Angebote im Internet zu finanzieren, das aber auf Kosten der Privatsphäre von Millionen von Menschen geht und Reichweite statt Qualität belohnt. Hunderte Unternehmen haben dafür ein undurchsichtiges System geschaffen – auch weil Gesetzgeber, Verlage und Werbetätige kein transparentes, faires und qualitätsförderndes Finanzierungsmodell für Journalismus und andere publizistische Tätigkeiten entwickelt haben. Damit die Hand des Überwachungskapitalismus möglichst unsichtbar bleibt, muss sie sorgsam hinter Marketing-Sprech, abweisenden Geschäfts- und Datenschutzbestimmungen und undurchschaubaren Technik- und Firmenstrukturen verborgen werden – denn sie agiert gegen geltendes Recht.

Wer im Internet unterwegs ist und sich nicht hauptberuflich mit den Praktiken der Werbeindustrie beschäftigt, hat keine Chance herauszufinden, wer welche Informationen zu welchem Zweck über sie oder ihn besitzt und ausnutzt.

Diese Undurchdringlichkeit muss technisch, juristisch und ökonomisch aufgeklärt werden – dazu gehört aber auch, die Betroffenen zu informieren. Wer Werbung im Internet sieht, muss wissen: Bei der Versteigerung von Werbeanzeigen werden umfangreiche persönliche Daten täglich millionenfach unkontrollierbar durch das Internet gespült. Das betrifft Daten wie Browserverlauf, Standort, eindeutige ID-Codes und Segmentierung nach sehr persönlichen Aspekten, zum Beispiel Einkommensklasse, politische oder sexuelle Orientierung. Dies widerspricht klar der EU-Datenschutzgrundverordnung.

Warum sind Verlage und Medien entscheidend?

Journalismus und andere publizistische Tätigkeiten werden im Internet zumindest teilweise durch „Lousy Pennies“ aus Werbeanzeigen finanziert, wie es Verleger Hubert Burda auf einer Digital-Konferenz 2009 formulierte. Weil Werbung stört, selten interessiert und, wenn ziellos verbreitet, wenig einbringt, verkauft die Werbeindustrie zielgruppengenaue Ansprachen. Werbende argumentieren, dass in ihrem Geschäft persönliche Daten und Aufmerksamkeit gegen Inhalte getauscht werden, die ansonsten mit Geld bezahlt werden müssten, wofür zu wenige Menschen bereit seien. Digitalcourage argumentiert, dass dieses Tauschgeschäft die Bedingungen des marktwirtschaftlichen Handels verlässt, weil das Grundrecht auf Privatsphäre keine handelbare Ware ist. Dieses Geschäft ist unverhältnismäßig. Die Öffentlichkeit gewöhnt sich daran, ständig beobachtet zu werden; Grundrechte werden ausgetreten; Medien orientieren sich an den Ansprüchen der Werbeindustrie statt anders herum und Werbetreibende werden zu Überwachern, ob sie wollen oder nicht.

Verlage und Medien sollten ein neues Geschäftsmodell erstreiten, denn es liegt im Interesse des anspruchsvollen Journalismus, dass sich die Leser-, Hörer- und Zuschauerschaft unbeobachtet informieren und austauschen kann. Wem die Unabhängigkeit und der Anspruch von Journalismus wichtig ist, sollte anerkennen, dass die Werbeindustrie mehr Probleme einbringt als Lösungen anbietet. Im Juni 2019 hat Zeit Online stellvertretend für viele andere Online-Medien einen BigBrotherAward bekommen, unter anderem für Werbetracker und den Facebook-Pixel. Laudator padeluun:

„Ihr nutzt Trackingtechniken von DoubleClick und erklärt gleich mal in der Datenschutzerklärung, dass Ihr auch nicht genau wisst, was Google mit den erfassten Daten macht. Und da ist der ‚DoubleClick Bid Manager‘ – das ist doch jetzt die ‚Google Marketing Platform‘, wo alles noch besser miteinander verzahnt ist und Google Analytics (das erwähnt Ihr zwei Seiten weiter) noch tiefer eingewoben ist. Und man kann

sich mit einem Facebook-Login bei Euch einloggen. Und da ist auch das Facebook-Pixel: Ihr verratet Facebook, wer Eure Leserinnen und Leser sind. Und zwar alle! Auch, die, die bewusst keinen Account bei den Datenverbrechern von Facebook haben."[2]

Wir wollen die Auseinandersetzung mit einer These, und die lautet: Dem anspruchsvollen Journalismus geht es besser ohne die kleinen Zuckerstückchen der datenhungrigen „Annoying-Industrie". Die Datenschutzverstöße durch Real Time Bidding sind eine Angelegenheit der Rechtsdurchsetzung. Der Mahlstrom aber, in dem sich Verleger und journalistische Online-Medien den Bedingungen und Gesetzen der Werbeindustrie anpassen, anstatt die Geschäftsmodelle den Ansprüchen und Herausforderungen der Informationsgesellschaft anzupassen, ist insbesondere eine Angelegenheit von Verlagen und Medien. Im Wettrennen um Aufmerksamkeit, Werbeplätze, Klicks und Daten drohen Inhalte, Komplexität und Hartnäckigkeit unterzugehen. Ersteres ist die eigentliche Ware, letzteres lediglich der Köder.

Wo ist der trackingfreie Werbeserver?

In der Auseinandersetzung mit kommerzieller und auch staatlicher Überwachung fragt Digitalcourage die Verantwortlichen häufig, ob Alternativen geprüft wurden und wenn ja, mit welcher Methode und welchen Ergebnissen. Meistens erhalten wir auf diese Frage keine Antworten – das sagt viel. Werbetreibende, Verlage und Regulierer sollten sich mit Blick auf die internationale Beschwerde gegen Real Time Bidding systematisch um datenschutzfreundliche, transparente und faire Alternativen bemühen.

Auf der Suche nach einer Möglichkeit, eine datenschutzfreundliche Anzeige für Digitalcourage zu schalten, haben wir exakt eine Nachrichtenseite gefunden, deren Anzeigenabteilung nachvollziehen konnte, dass wir unsere Leserschaft nicht an Google-Werbe-Server ausliefern wollen. Nur ein Medium war bereit, Werbung hauptsächlich auf den eigenen Servern laufen zu lassen. Alle anderen Medien nutzen die vollen Werbe- und Tracking-Produktpalette von Google und Co., wobei Google eine monopolähnliche Schlüsselrolle innehat.

Warum betreiben Online-Medien keine trackingfreien Werbeserver nach ihren eigenen Regeln und Bedürfnissen? Unser Appell lautet: Weniger Zeit, Geld und Intellekt in die eigene Anpassung an „soziale Medien" und Werbemechanismen investieren – sondern unabhängige Strukturen aufbauen, die sich an Inhalten oder dem Interesse von Kund.innen an Produktinformationen orientieren und nicht an privaten Daten.

Beschwerde eingereicht – wie geht es weiter?

Die Beschwerde gegen Real Time Bidding wurde in 16 Ländern eingereicht, wobei sie von einigen nationalen Aufsichtsbehörden zum irischen Datenschutzbeauftragten weitergeleitet wurde. Der britische Datenschutzbeauftragte (ICO) hat einen Bericht zu RTB vorgelegt, in dem klargestellt wird, dass die Praktiken mit Datenschutzrecht kollidieren, und den Verantwortlichen sechs Monate eingeräumt, ihre Praktiken entsprechend zu ändern. Seit Juli 2019 sammelt der ICO weitere Informationen über die Sicherheit von persönlichen Daten, Profilbildung und zu der Frage, ob eine Datenschutz-Folgenabschätzung erstellt wurde.[3] Nach sechs Monaten, also im Januar 2020, erwägt der ICO eine Kontrolle der Werbeindustrie und wird gegebenenfalls die Unternehmen um eine Neubewertung ihres Umgangs mit persönlichen Daten bitten.

Die Civil Liberties Union und in Deutschland die Digitale Gesellschaft, das Netzwerk Datenschutzexpertise, die Deutsche Vereinigung für Datenschutz und wir von Digitalcourage werden diese Zeit nutzen, um Menschen darüber aufzuklären, wie die Werbeindustrie mit ihren persönlichen Daten umgeht. Wir würden uns sehr freuen, wenn sich Jurist.innen, Datenschutzexpert.innen, Journalist.innen und Techniker.innen an der Kampagne #StopSpyingOnUs beteiligen und mit ihrer Expertise helfen, das Werbetreiben im Internet an dieser Stelle zu reparieren. Für Redaktionen und Verlage ist dieser Diskurs die Chance, ihre für die Gesellschaft entscheidende Arbeit auf ein wertigeres und stabileres Fundament umzuziehen.

Wir wollen und brauchen anspruchsvollen, unabhängigen und fair bezahlten Journalismus.

1 https://www.liberties.eu/de/news/quiz-real-time-bidding-de/17726

2 Text: https://bigbrotherawards.de/2019/verbraucherschutz-zeit-online

Video: https://media.ccc.de/v/bigbrotherawards2019-23423-die-oscars-fuer-ueberwachung#t=5946

3 https://fixad.tech/a-summary-of-the-ico-report-on-rtb-and-what-happens-next/

Reaktionen

Im Rahmen der Kampagne zum Real Time Bidding haben wir die beiden Hauptbetreiber dieser Werbetechnik in Deutschland, also Google sowie die Vertretung von IAB Europa, den Bundesverband Digitale Wirtschaft (BVDW), angeschrieben und sie um Stellungnahmen gebeten. Wir haben insbesondere folgende Fragen gestellt:

- Was ist geplant, die Standards von RTB so gestalten, dass dieses Angebot dem Datenschutzrecht entspricht?
- Wie sollen insbesondere die schutzwürdigen Betroffeneninteressen berücksichtigt werden?
- Was ist geplant, um die Nutzenden über das Real Time Bidding (RTB) sowie über deren Rechte hierbei zu unterrichten?
- Welcher Zeitplan besteht, um beim RTB rechtskonforme Zustände herzustellen?

Beide Institutionen antworteten auf unsere Anfrage. Während der BVDW sich inhaltlich zu einigen rechtlichen Details äußerte, nicht aber zu Fragen des Betroffenenschutzes, machte Google

hierzu sehr allgemeine Aussagen, dafür aber keine Mühe einer rechtlichen Einordnung.

Stellungnahme von Google vom 01.08.2019

Vielen Dank für Ihre Anfrage vom 30. Juni. Hierzu möchte ich Ihnen die unten stehende Stellungnahme schicken.

- *We've welcomed European regulators' encouragement of clear rules for online advertising. The industry needs more guidance on real-time bidding.*
- *Google has a particular interest in supporting a healthy online environment that users trust. Our ability to provide access to high-quality, trusted, and useful information by promoting the continued viability of publishing on the web — a goal that supports the long-term interests of publishers and Google alike — is hindered if we don't take robust measures to protect the data of our users.*
- *Authorized Buyers using our systems are subject to stringent policies and standards.*

For example:
We set one of the highest standards amongst industry for user transparency and consent for personalised advertising. We ask our users for their consent to use data for personalised ads, and ask our customers who use our products to comply with strict policies which require they obtain consent for personalised advertising from visitors to their sites & apps.
We take significant measures so as not to share web visitors' precise location, while still giving ad buyers assurance that locally-relevant ads are being seen locally; in order to do this,

- *We truncate IP addresses that are sent as part of bid requests by deleting the last several digits*
- *We provide only a coarse location (for example, a neighborhood) and never the specific location of the user*
  We don't share location histories nor inferences about users' interests based on their activity
  We prevent the targeting by advertisers of overly narrow or specific audiences as a matter of policy (for advertising or for data collection)
  We give users a persistent opt-out from personalised advertising both at the level of the account and user device: we don't send user information that's pertinent for bid requests at all if the user opts out.

- *In addition, we provide leading industry tools providing users with transparency into how data is used in real time via "Why this Ad". We also provide transparency to users on what data Google saves about them in their Google Account, where users can view and manage their data, privacy, and security settings. Users can go to their ad settings to control the use of data for ads personalization and for all ads shown by Google.*
- *We recognize that the real-time bidding process is currently under examination by a number of data protection authorities.*
  - *We are engaging fully with the Irish Data Protection Commissioner's investigation and have welcomed the UK Information Commissioner's Office's guidance.*
  - *While we cannot comment on an ongoing investigation nor prejudge the outcomes of these processes, we are committed to engaging with regulators and others in the advertising industry to promote outcomes that protect users and help keep the open web sustainable and free.*

Es war also Google nicht wert, auf eine deutschsprachige Anfrage eine deutschsprachige Antwort zu geben. Vielmehr besorgte sich Google Deutschland offenbar aus Irland (oder gar aus den USA) eine englischsprachige Antwort, die einfach weitergegeben wurde. Hier unsere Übersetzung:

„- Wir haben die Ermutigung der europäischen Aufsichtsbehörden begrüßt, klare Regeln für die Internet-Werbung aufzustellen. Die Industrie benötigt nähere Hinweise zum Real Time Bidding.
- Google hat ein besonderes Interesse daran, dass eine gesunde Online-Umgebung entwickelt wird, der Nutzende vertrauen. Unsere Fähigkeit, Zugang zu hochqualifizierten, vertrauenswürdigen und nützlichen Informationen zu verschaffen, indem wir die dauernde Leistungsfähigkeit von Webveröffentlichungen fördern – was sowohl im Langzeitinteresse der Veröffentlicher wie von Google liegt – wird beeinträchtigt, wenn wir keine nachdrücklichen Maßnahmen zum Schutz der Daten unserer Nutzer ergreifen.
- Authorized Buyers, die unser System nutzen, unterliegen strengen Vorgaben und Standards.

Zum Beispiel:
Wir setzen mit die höchsten Industriestandards für Nutzertransparenz und Einwilligungen bei personalisierter Werbung ein. Wir bitten unsere Nutzenden um ihre Zustimmung für die Verwendung der Daten für personalisierte Werbung und wir verlangen von unseren Kunden, die unsere Produkte einsetzen, den strengen Regeln zu entsprechen, die ihnen Einwilligungen der Besucher ihrer Seiten und Anwendungen für personalisierte Werbung abverlangen.
Wir ergreifen beachtliche Maßnahmen, etwa zur Vermeidung des Teilens der genauen Lokalisierung der Netzbesucher, und geben zugleich den Werbekunden die Zusicherung, dass örtlich relevante Werbung örtlich zur Kenntnis gegeben wird. Hierfür

- verkürzen wir die IP-Adressen, die als Teil der Gebotsanfragen weitergegeben werden, indem wir die letzten Ziffern löschen,
- liefern wir nur eine grobkörnige Ortsangabe (z. B. einer Nachbarschaft) und niemals den präzisen Aufenthalt des Nutzenden.

Wir teilen weder das Bewegungsprofil noch Abweichungen bzgl. der aus den Aktivitäten abgeleiteten Nutzerinteressen.
Wir verhindern durch unsere Vorgaben (für Werbe- oder Datensammlzwecke) zielgenaue Ansprachen durch Werbende bei zu engen und spezifischen Gruppen.
Wir ermöglichen den Nutzenden ein jederzeitiges Opt-out von personalisierter Werbung sowohl auf der Ebene des Nutzerkontos wie des genutzten Geräts: Wir senden überhaupt keine Nutzerinformationen, die für Gebotsanfragen relevant sind, wenn der Nutzer ein Opt-out erklärt.

- Außerdem stellen wir in der Branche führende Instrumente über „Why this Ad?“ zur Verfügung, mit denen Nutzenden transparent gemacht wird, wie die Daten in Echtzeit genutzt werden. Wir verschaffen Nutzenden auch Transparenz darüber, was Google über sie in ihrem Google-Konto speichert, wo diese die Daten, den Datenschutz und die Sicherheitseinstellungen einsehen und verwalten können. Die Nutzenden können zu ihren Werbeeinstellungen gelangen, um die Nutzung der Daten für personalisierte Werbung und für alle von Google angezeigten Werbeeinblendungen zu kontrollieren.
- Wir erkennen an, dass das Verfahren des Real Time Bidding momentan von mehreren Datenschutzaufsichtsbehörden überprüft wird.
  - Wir kooperieren vollständig bei den Untersuchungen der irischen Datenschutzaufsichtsbehörde und haben die Richtlinien der britischen Datenschutzaufsichtsbehörde begrüßt.
  - Wir können weder die laufende Untersuchung kommentieren noch die Ergebnisse dieser Verfahren vorhersagen und bewerten, bekennen uns aber dazu, mit den Aufsichtsbehörden und Anderen in der Werbeindustrie zusammenzuarbeiten, um Ergebnisse zu erzielen, die die Nutzenden schützen und die dabei helfen, das offene Netz funktionstüchtig und frei zu halten.“

Stellungnahme des Bundesverbandes Digitale Wirtschaft (BVDW) e.V.

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle vertritt der BVDW die Interessen der Digitalen Wirtschaft gegenüber Politik und Gesellschaft und setzt sich für die Schaffung von Markttransparenz und innovationsfreundlichen Rahmenbedingungen ein.

Wir nehmen gerne die Möglichkeit wahr, zur Diskussion über die Beschwerde verschiedener NGOs vom 4. Juni 2019 beizutragen und deren Schwachstellen transparent zu machen. Wir beschränken uns dabei auf die Ausführungen zum IAB Transparency & Consent Framework (IAB TCF) und zum IAB OpenRTB Standard (OpenRTB), können aber keine Aussagen zu dem proprietären RTB-System „Authorized Buyers“ treffen.

Bedauerlich ist zunächst, dass sich die NGOs darauf beschränken, den neun Monate zuvor veröffentlichten „Ryan-Report“ vom September 2018 ins Deutsche zu übersetzen, ohne ihn zumindest zu aktualisieren. So beziehen sich die Beschwerdeführer nach wie vor auf das IAB TCF in der Ursprungsversion, obwohl die wesentlich geänderte Nachfolgeversion v2.0 bereits seit mehr als einem Monat veröffentlicht war. Die Beschwerdeführer belasten die Aufsichtsbehörden insofern fahrlässig mit einem überholten Sachvortrag – dies hätte sich bei einer sorgfältigeren Befassung mit der Materie leicht vermeiden lassen.

Sowohl den Beschwerden als auch dem „Ryan-Report“ werden teilweise fehlerhafte Sachverhalte, teilweise fehlerhafte Rechtsinterpretationen mit Blick auf das Übertragungsprotokoll OpenRTB als auch auf das derzeit in der Entwicklung befindliche TCF des IAB Europe zugrunde gelegt.

1. Bei OpenRTB handelt es sich um einen Übertragungsstandard ähnlich wie z.B. das Hypertext Transfer Protokol (HTTP). Hierüber können Daten ohne Ansehung ihrer Qualität oder sonstiger Eigenschaften für sektorspezifische Anforderungen der heutzutage automatisiert (programmatisch) stattfindenden Werbemittelauslieferungen in einem marktübergreifend akzeptierten Format übertragen werden.

Ein solches Protokoll ist das Gerüst, nicht aber selbst Gegenstand einer Verarbeitungstätigkeit im Sinne der DSGVO. Aus diesem Grunde ist das im „Ryan-Report“ bzw. unter Bezugnahme auf einen entsprechenden Brief an das IAB Tech Lab zitierte Fanpage-Urteil des EuGH in seinen Feststellungen zur Frage der verantwortlichen Stelle schon nicht einschlägig. Ein technischer Standard wie das OpenRTB-Protokoll bietet keine eigene Entscheidungsmöglichkeit über die Zwecke und Mittel der Datenverarbeitung bei einer anderen, das Protokoll einsetzenden, verantwortlichen Stelle.

Die Behauptung, dass OpenRTB gegen die DSGVO bereits deswegen verstoße, weil Unternehmen es rechtswidrig nutzen könnten, stünde außerdem der Behauptung gleich, dass auch das zugrunde liegende Hypertext Transfer Protocol („HTTP“) gegen die DSGVO verstößt. Mit einer solchen Argumentation könnte man alle möglichen Internettechniken „verantwortlich“ für individuelle Verarbeitungsentscheidungen machen. Eine Folge übrigens, die laut den Schlussanträgen im Fall FashionID ausdrücklich ausgeschlossen sein soll. Denn die „Ermöglichungs-Kette“ könne ansonsten theoretisch bis hin zum Stromanbieter reichen.

2. Im „Ryan-Report“ - der sich auf die veraltete Vorgängerversion 1.0 bezieht - wird behauptet, das TCF würde über OpenRTB Daten wie bei einer Rundfunksendung an eine unüberschaubare Anzahl von Akteuren „broadcasten“. Das ist unrichtig. Das TCF ist selbst keine Werbedaten(übertragungs)plattform, sondern steuert die Zuordnung von vorab definierten Verarbeitungszwecken zu den jeweiligen Akteuren und deren Rechtsgrundlagen über einen verbindlichen Signalstandard (sog. Consent-String). Dieser ermöglicht die technische Zuordnung von Signalen an eine fest definierte Gruppe, die verbindlichen Verarbeitungsregeln unterliegt.

Anliegen und Hintergrund des TCF ist es gerade, Transparenz bezogen auf die beteiligten Akteure im Markt herzustellen. Über die Consent Management Platform (CMP) werden nur die Akteure dargestellt, die von der CMP und damit inklusive der von ihnen angegebenen – fest vorgegebenen – Verarbeitungszwecke ausgewählt und damit identifizierbar gemacht wurden. Das Framework standardisiert über die entsprechenden Schnittstellen und den Consent-String also, wie Transparenz hergestellt und die Informationen über eingeholte Einwilligungen weitergegeben werden. Mit Blick auf die Verwendung von OpenRTB wird folglich auch die „Verbreitung“ der Daten gesteuert. Alle Akteure sind über die TCF-Policy verpflichtet, eine Verarbeitung zu unterlassen, soweit eine geeignete Rechtsgrundlage fehlt. Aus

dem Katalog der Verarbeitungszwecke ergibt sich dann auch der Einsatzbereich des Frameworks. Anders als im „Ryan-Report" dargestellt, werden Verarbeitungen sensibler personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO gar nicht erst vom TCF erfasst.

Berlin, 26. Juli 2019
Ansprechpartner RA Michael Neuber, Justiziar/Bereichsleiter Politik und Recht

Die Debatte ist eröffnet. Die Aufsichtsbehörden sind eingeschaltet und stehen in der Pflicht, eine technische und eine rechtliche Bewertung abzugeben. Aus den oben abgedruckten Antworten von Google und des BVDW zeigt sich, dass sowohl die technische wie auch die rechtliche Bewertung jeweils differenziert erfolgen muss: Während Google seine Verantwortlichkeit gar nicht leugnet, verschiebt der BVDW die datenschutzrechtliche Verantwortung auf die Internet-Veröffentlicher. Google benennt Schutzmaßnahmen für die Betroffenen, doch bleiben diese im Vagen und erreichen die Betroffenen nicht bzw. können sie nicht erreichen. RTB wird so zu einem exemplarischen Fall, wie die DSGVO in Sachen Transparenz und Wahlfreiheit in Zukunft umgesetzt wird. RTB könnte die Blaupase dafür werden, welche Anforderungen die Datenschutzbehörden in Bezug auf „Privacy by Default" (Art. 25 Abs. 2 S. 3 DSGVO) stellen. Es bleibt spannend.

Thilo Weichert

Ahnenforschung mit Gendaten

Der BigBrotherAward 2019 in der Kategorie Biotechnik geht an **die Firma Ancestry.com**

mit ihrer Niederlassung in München, weil sie das Interesse an Familienforschung dazu ausnutzt, Menschen zur Abgabe von Speichelproben zu veranlassen.

Familienforschung – auch Ahnenforschung oder Genealogie genannt – ist ein relativ harmloses Hobby: Wer bin ich? Wo komme ich her? Mit wem bin ich verwandt? Diese Fragen wurden früher mit Geburts-, Heirats- und Sterbeurkunden, Familienstammbäumen und Kirchenbüchern beantwortet. Die Gentechnik eröffnet nun ganz neue Erkenntnismöglichkeiten, da die Analyse unserer Gene, unserer DNA, verrät, mit wem wir biologisch verwandt sind – bis zum 3. oder 4. Grad. Selbst die sogenannte biogeografische Herkunft unserer Urahnen, also die Frage, in welcher Region meine Familienmitglieder in vergangenen Generationen gelebt haben, lässt sich mit einer gewissen Wahrscheinlichkeit genetisch bestimmen.

DNA ist die englische Abkürzung für Desoxyribonukleinsäure - deoxyribonucleic acid – die wissenschaftliche Bezeichnung für unser Genom, also die Gesamtheit unserer Erbanlagen. Die Erkenntnisse daraus sind verblüffend. Kein Wunder, dass viele Familienforschende ihren Speichel zur Untersuchung einsenden, um mehr über sich herauszubekommen.

Familienforschung als Hobby ist in den USA weit verbreitet. Viele Firmen bieten hierzu ihre Dienste an. Der Marktführer ist Ancestry.com mit angeblich derzeit mehr als 10 Millionen Kund.innen weltweit und 20 Milliarden weiteren Datensätzen und Urkunden, gefolgt von der Google-Gründung „23andMe" mit 5 Millionen DNA-Analysen[1].

Ancestry hat in München eine Niederlassung eingerichtet und drängte kurz vor Weihnachten 2018 massiv auf den deutschen Markt. Versprochen wird eine „Selbstentdeckungsreise", „Erstaunliches über sich selbst", ein „Schlüssel in die Vergangenheit". Das Ganze für einen Einführungspreis von 79 €, heute 89 € incl. Mehrwertsteuer zuzüglich Versand. Ein Schnäppchen, denn immerhin hat im Jahr 2003 die erste Entschlüsselung des gesamten menschlichen Genoms mit seinen über 3 Milliarden Basenpaaren im Rahmen des Human Genome Projects noch 3 Milliarden Euro gekostet. 2008 fielen die Kosten pro Genom auf eine Million Euro. 2011 war ein Next Generation Sequencing schon für 10.000 € zu haben. Ein Jahr später konnte erstmals das 1000-Euro-Genom mit der inzwischen verfügbaren Rechenpower und neuen Analysemethoden innerhalb weniger Stunden analysiert werden.

Das Angebot ist nicht nur „billig", sondern auch einfach zu bekommen: Im Internet kann ich ein Ancestry-Konto einrichten und mir damit ein Testkit bestellen. Meine Speichelprobe wird an ein Labor geschickt; 6 bis 8 Wochen später kann ich im Internet über den Account die Ergebnisse abrufen. Toll!

Dass da alles mit guten Dingen zugeht, dafür verbürgten sich angeblich Ende 2018 auf der Internetseite von ancestry.com noch viele deutschsprachige „Partner", etwa viele Landesarchive, die Deutsche Nationalbibliothek, das Deutsche Auswandererhaus, die Marineschule Mürwik, das Schweizerische Bundesarchiv oder der niedersächsische Landesverein für Familienkunde. Nur: Von uns auf ihre Partnerschaft angesprochen, hatten diese davon keine Ahnung. Schnell verschwand dann auch diese illegale Werbemethode.

Das Angebot sei, so heißt es auf der Internetseite, datenschutzkonform. „Sicherheit und Datenschutz genießen bei Ancestry oberste Priorität". Die Kunden blieben „Eigentümer ihrer Daten". Die Daten sowie die Gewebeproben würden auf Anforderung der Betroffenen wieder gelöscht bzw. vernichtet. Eine Weitergabe an Dritte erfolge nicht – außer, soweit „gesetzlich erforderlich" oder „Sie geben uns Ihre ausdrückliche Zustimmung". Also alles paletti?

Der Haken liegt – wie so oft – im Kleingedruckten und ist im Falle von

Ancestry in einem dichten Gestrüpp von Bestimmungen verborgen: einer 16seitigen Datenschutzerklärung[2], elf Seiten Allgemeine Geschäftsbedingungen[3] und siebeneinhalb Seiten Einwilligung in das Forschungsprojekt „Ancestry Human Diversity Project"[4].

Mit dem Einsenden des Speichels erfolgt die Zustimmung zu den Datenschutzbestimmungen, wonach Ancestry selbst mit meinen Daten unbeschränkt über „Merkmale, persönliche Gesundheit und persönliches Wohlbefinden" Forschung durchführen kann. Wird dem „Ancestry Human Diversity Project" zugestimmt, so kommen „mitwirkende Partner" ins Spiel. Die Partner befinden sich „in den Vereinigten Staaten und anderen Ländern". Dabei kann es sich um „akademische Einrichtungen sowie Non-Profit-Organisationen, gewinnorientierte Unternehmen und Regierungsbehörden" handeln.

Wer in dieses „Ancestry Human Diversity Project" einmal seine Einwilligung erteilt, gibt die Kontrolle über seine genetischen Daten aus der Hand und hat keinen Einfluss mehr darauf, wer was und wo damit forscht. Ca. 80% der Einsendenden geben gemäß Presseberichten bei 23andMe ihre DNA für „Forschungszwecke" frei und machen weitere Angaben zu sich und ihrer Familie[5]. Bei Ancestry dürfte es ähnlich sein.

Damit nicht genug: Den Kunden als „Eigentümern ihrer Daten" wird von Ancestry jegliche Auskunft verweigert über die sogenannte Forschung, über Methoden, Partner oder Rückschlüsse, die daraus gezogen werden. Was dahinter steckt, wird offenkundig, wenn man sich die junge, aufstrebende Branche der Gendatenkraken genauer ansieht. So schloss der Ancestry-Konkurrent 23andMe, der nur einen halb so großen Datenbestand hat, kürzlich mit dem Pharmakonzern GlaxoSmithKline über 300 Mio. US-Dollar einen Kooperationsvertrag zur Nutzung der Daten. Das Geschäftsmodell dieser Anbieter ist nicht die Ahnenforschung, sondern es geht um das ganz große Geld mit den Gendaten, mit insbesondere der Pharmaindustrie als Abnehmer.

Das Ganze ist also keine Win-Win-Geschichte, bei denen Kunden einfach für eine Dienstleistung bezahlen, die sie bestellt haben. Tatsächlich werden die Betroffenen abgezockt. Die Abzocke erinnert an Google, Facebook und Co. mit Internetdaten. Die Betroffenen erhalten außer spärlichen Auswertungsergebnissen keine Auskunft über die Nutzung ihrer Daten, geschweige denn, dass sie – als vermeintliche „Dateneigentümer" – an den Gewinnen beteiligt würden. Im Gegenteil: Ihnen wird von Ancestry gar verboten, ihre eigenen Analyseergebnisse an Dritte weiterzugeben[6].

Welche weiteren Begehrlichkeiten die Daten der Firma Ancestry wecken, ist 2018 aus den USA bekannt geworden. Menschen, die dort ihre DNA analysieren ließen, gerieten mitsamt ihren Familien ins Visier der Polizei, etwa weil sie mit dem so genannten „Golden State-Killer" auch nur entfernt verwandt sind. Um den Täter zu ermitteln, wurde die gesamte Verwandtschaft von den Ermittlern ausgeforscht. Kein Wort bei Ancestry über die potenzielle Strafverfolgung von biologischen Verwandten.

Ancestry erteilt deutschen Kunden vor der DNA-Analyse auch keine humangenetische Beratung, obwohl diese verpflichtend im deutschen Gendiagnostikgesetz vorgesehen ist. Die Firma prüft auch nicht, ob eine Person berechtigt ist, die eingesendeten Speichelproben untersuchen zu lassen. So könnte z. B. ein Vater DNA von sich und von seinen Kindern einsenden, um auf diesem Weg de facto einen Vaterschaftstest machen zu lassen. Ancestry klärt ihn weder darüber auf, dass er sich damit nach deutschem Recht strafbar macht, noch dass seine biologischen Verwandten ein „Recht auf Nichtwissen" haben und welche gravierenden familiären Verwerfungen und psychischen Folgen so ein Schritt haben kann, etwa wenn per DNA-Test die Unehelichkeit eines Kindes herauskommt oder ein angeblich anonymer Samenspender plötzlich ans Tageslicht gezerrt wird.

Nichts gegen Genanalysen. Diese können für die Familienforschung, insbesondere aber für die Medizin eine wichtige Erkenntnisquelle sein. Doch sollten die Probengeber sich darüber im Klaren sein, was sie da tun. Anbieter wie Ancestry missbrauchen das Interesse an Familienforschung, um einen Genom-Schatz für die kommerzielle Forschung anzuhäufen, denn das ist ihr eigentliches Geschäftsmodell. Die Datenschutzrechte der Probengeber und ihrer Verwandten müssen respektiert werden. Die deutschen Datenschutz- und Aufklärungspflichten werden aber von Ancestry aus Profitinteresse bewusst ignoriert. Wir sehen hier einen Trend: Nach der Ausbeutung von Internetdaten wird die Ausbeutung von Gendaten das nächste ganz große Ding. Ancestry ist der Platzhirsch, der keine Datenschutz- oder Grundrechtsskrupel kennt.

Deshalb erhält Ancestry den BigBrotherAward 2019. Herzlichen Glückwunsch.

1 https://www.consumerreports.org/health-privacy/how-to-delete-genetic-data-from-23andme-ancrestry-other-sites/

2 https://www.ancestry.de/cs/privacyphilosophy

3 https://www.ancestry.de/cs/legal/termsandconditions

4 https://www.ancestry.de/dna/lp/informedconsent-v4-de

5 http://www.bbc.com/capital/story/20190301-how-screening-companies-are-monetising-your-dna

6 Allgemeine Geschäftsbedingungen von Ancestry, https://www.ancestry.de/cs/legal/termsandconditions, Punkt 2

URL der Laudatio: https://bigbrotherawards.de/2019/biotechnik-ancestry_com

Auf die Laudatio gab es in einem Blog am 11.06.2019 eine prompte Reaktion mit dem Titel „Fakenews über Ancestry-DNA" von einem Tobias A. Kemper, die unter „https://saecula.de/fakenews" veröffentlicht wurde. Dies veranlasste Thilo Weichert zu folgender Erwiderung:

BigBrotherAward an Gen-Analyse-Firma ist Fakenews?

Nicht erst seit Donald Trump ist es eine weit verbreitete Praxis, dass man versucht, die berechtigte öffentliche Kritik an kontrovers diskutierten Fakten als Fakenews zu diskreditieren. So auch bei der „Widerrede in zwölf Punkten" von Saecula, mit der auf meine Laudatio bei den BigBrotherAwards 2019 zu Ancestry DNA reagiert wird.

Ich begrüße diese Widerrede ausdrücklich, da sie Anknüpfungspunkt für eine öffentliche Debatte zu genetischer Genealogie generell und zum Angebot von Ancestry speziell sein kann. Diese

öffentliche Debatte hätte schon kurz vor Weihnachten 2018 erfolgen können, als das Netzwerk Datenschutzexpertise am 17.12. das 34-seitige Gutachten „AncestryDNA ist in Deutschland" veröffentlicht hat. Das Gutachten wurde Ancestry vorab am 2.12.2018 mit der Bitte um Stellungnahme sowie um Bereitstellung weiterer datenschutzrelevanter Unterlagen (Datenschutz-Folgenabschätzung, Standardvertragsklauseln) zugesendet. Nach einer Eingangsbestätigung und trotz Mahnungen hat Ancestry auf meine Anfrage bis heute nicht inhaltlich geantwortet. Vielmehr wurde auf die Internetveröffentlichungen verwiesen, die gerade Anlass meiner Kritik waren und sind. Auch Anfragen von dritter Seite, selbst von Stellen, mit denen Ancestry zunächst wettbewerbswidrig als Partner geworben hatte, wurden – soweit mir bekannt – inhaltlich von Ancestry nicht beantwortet.

Vorab einige Klarstellungen zu meiner Person:

- Falsch ist, dass ich 2008 behauptet hätte, dass Google Street View „Einbrechern" helfen würde. Richtig ist, dass ich als Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein darauf hingewiesen habe, dass Googles Angebot „Street View" gegen Datenschutzregeln verstößt, was das Unternehmen dazu veranlasste, bundesweit Sicherungsmaßnahmen zuzusichern und vorzunehmen (Verpixelung, Einräumung eines Widerspruchsrechts).
- Falsch ist, dass ich 2010 eine „Ausweispflicht für Internetbenutzer" gefordert hätte. So einen Unsinn würde ich nie vorschlagen, geschweige denn fordern. Richtig ist vielmehr, dass ich mich seit vielen Jahren dafür einsetze, dass das Internet anonym genutzt werden kann.
- Falsch ist, dass ich 2012 „das Ende von Facebook wegen dessen Umgang mit dem Datenschutz" vorausgesagt hätte. Richtig ist, dass das Angebot von Facebook gegen den Datenschutz verstößt, was inzwischen von vielen Gerichten bestätigt wurde. Richtig ist, dass ich gegen das Ende von Facebook nichts einzuwenden hatte und auch weiterhin habe, solange dieses Unternehmen Nutzerdaten unrechtmäßig verarbeitet.

Punkt 1: Ich habe absolut nichts gegen Ahnenforschung. Im Gegenteil: Auch ich finde es interessant, mehr über meine Vorfahren zu erfahren. Es gibt aber Ahnenforschung, die moralisch und evtl. auch rechtlich nicht in Ordnung ist. Es kommt auf die Zielsetzung und die Methoden an. So dürfte unbestreitbar sein, dass die Ahnenforschung während der Zeit des Nationalsozialismus „zu Ausgrenzung, Diskriminierung bis hin zur Ermordung von Angehörigen ethnischer Minderheiten" eingesetzt wurde. Wer dies leugnet, verharmlost auch heute noch weiterhin mögliche und stattfindende Diskriminierungen und die Verfolgung auf der Grundlage von einer genetischen Zuordnung zu Ethnien.

Punkt 2: Es ist nichts Anrüchiges, DNA-Analysen als gentechnische Verfahren darzustellen. Mit dem Begriff „Gentechnik" werden DNA-Analysen nicht „unterschwellig in ein schlechtes Licht" gesetzt. Vielmehr setze ich mich seit Jahren dafür ein, dass DNA-Analysen, also gentechnische Verfahren, im Bereich der medizinischen Forschung einfacher und besser genutzt werden können.

Punkt 3: Mir ist nicht erkennbar, was an meiner zweifellos verkürzten „Definition von DNA" „völlig unsinnig" sein soll. Es ist gerade ein Versprechen von Ancestry und anderen Unternehmen, über die DNA-Analyse Verwandtschaftsbeziehungen aufzufinden.

Punkt 4: Ende 2018 wurden die „Partner" unter https://www.ancestry.de/cs/de/partners dargestellt. Tatsächlich werden einige Partner inzwischen weiterhin, aber nicht mehr im Kontext von DNA-Analysen unter https://www.ancestry.de/cs/us/partners, präsentiert. Diese Änderung dürfte darauf zurückzuführen sein, dass ich die genannten „Partner" auf deren werbliche Verwendung hingewiesen habe und diese hiergegen bei Ancestry vorstellig wurden.

So teilte mir z. B. das Bundesarchiv mit Mail vom 07.01.2019 mit: „Die Zusammenarbeit zwischen dem Bundesarchiv und Ancestry steht in keinem Zusammenhang mit irgendwelchen Genanalysen."

Die deutsche Nationalbibliothek antwortete mir mit Mail vom 22.01.2019:

„Wir haben ... die Homepage von Ancestry überprüft und Fakten gefunden, die uns keineswegs begeistert haben: Neben der unberechtigten Nutzung unseres geschützten Logos wurden wir auch als „Partner" von Ancestry bezeichnet. Beide Maßnahmen waren nie mit unserem Hause abgestimmt gewesen. Mit Ancestry wurden bislang lediglich zwei Verträge zur Digitalisierung von Medien (Adressbücher) geschlossen; beide Maßnahmen, die zuvor mit dem BfDI datenschutzrechtlich abgestimmt waren, sind abgeschlossen. Die Deutsche Nationalbibliothek möchte unter allen Umständen vermeiden, mit der unberechtigten Kennzeichnung als Partner den Eindruck entstehen zu lassen, bei diesem Genanalysen-Angebot mit Ancestry zu kooperieren. Zwischenzeitlich haben wir Ancestry (nicht zuletzt wegen Ihrer Empfehlung) angeschrieben und aufgefordert, das Logo der Deutschen Nationalbibliothek sowie die irreführende Bezeichnung als „Partner" umgehend von der Homepage zu löschen."

Punkt 5: Es ist falsch, dass sich die BBA-Laudatio nicht zu „heiklen, fragwürdigen oder für den Nutzer nachteiligen Bestimmungen" in den Datenschutzbestimmungen, den allgemeinen Geschäftsbedingungen oder der Einwilligungserklärung von Ancestry äußert. Die Zitate sind in der Laudatio https://bigbrotherawards.de/2019/biotechnik-ancestry_com als solche gekennzeichnet und die nachteiligen Effekte dargestellt.

Folgende Aussage der „Widerrede" ist geradezu verstörend: „Die entsprechenden Abschnitte in seinem „Gutachten" mag ein Jurist auf ihre Stichhaltigkeit hin überprüfen". Das Gutachten wie die Laudatio verfolgt als Hauptanliegen, eine absolut illegale Form der Datenverarbeitung zu thematisieren. Zu diesem Hauptanliegen verweigert die „Widerrede" jede Stellungnahme. Die Durchsetzung der bestehenden Gesetze darf bei derart sensiblen Sachverhalten nicht als juristisches Klein-Klein abgetan werden.

Es mag richtig sein, dass die Ancestry-Konkurrenten FTDNA, My Heritage, 23andme oder Gedmatch.com mit ihrem Angebot weiter gehende Verstöße gegen Datenschutzrecht praktizieren. Richtig ist aber auch, dass Ancestry

der größte Anbieter ist und neben MyHeritage (https://www.myheritage.de) bisher der einzige, der sich mit seinem deutschsprachigen Angebot an deutsche Verbraucher wendet.

Punkt 6, 7: Es ist ein Irrtum, dass Nutzer durch „ausdrückliche Einwilligung" ihre Daten ohne Einschränkungen „für weitergehende Forschungen zur Verfügung" stellen können, da damit nicht nur eigene Daten, sondern auch die der nicht befragten Verwandten mit übermittelt werden.

Es ist nicht zutreffend, dass Ancestry „ausführlich über eventuelle Risiken" informiert. In der Laudatio werden einige der unterschlagenen Risiken (Unkontrollierbarkeit bei der Weitergabe an Dritte, Finanzinteresse von Ancestry, humangenetische Beratung, technische Möglichkeit eines Vaterschaftstest, Recht auf Nichtwissen der Verwandten, straf-/rechtliche Risiken für den Speicheleinsender) aufgeführt.

Da Ancestry bisher jede Stellungnahme zu den von mir gemachten Vorwürfen verweigert hat, liegen mir keine Angaben zu dem Unternehmen hinsichtlich erteilter Einwilligungen vor. Bekannt ist mir bisher auch nicht, welches Entgelt Dritte für die Nutzung von Daten an Ancestry bezahlen. Es ist kein Grund erkennbar, weshalb die zu 23andme bekannten Angaben nicht auf Ancestry übertragbar sein sollten. Ancestry steht es frei, zum eigenen Unternehmen genaue Zahlen zu nennen.

Punkt 8: Es ist richtig, dass Ancestry die Rohdaten aus den DNA-Analysen bereitstellt. Auch richtig ist, dass es dadurch Nutzenden technisch möglich ist, diese Daten Dritten zur Verfügung zu stellen. Vermutlich, um aber genau dies zu verhindern, hat Ancestry in die Vertragsbedingungen ausdrücklich ein Weitergabeverbot aufgenommen. Den Nutzenden wird Vertragsbrüchigkeit angedroht, wenn sie die erlangten „Inhalte und Informationen" weitergeben. Dies ist nicht mit der Behauptung in Einklang zu bringen, die Nutzer seien „Eigentümer" der Daten.

Punkt 9: Richtig ist, dass der „Golden-State-Killer" durch einen Datenabgleich bei Gedmatch.com gefunden wurde; richtig mag auch sein, dass Ancestry kein Hochladen von Rohdaten anderer Anbieter durch Nutzer gestattet. Etwas anderes wurde auch nicht in der Laudatio behauptet. Richtig ist aber auch, dass von Ancestry keine wirksamen Maßnahmen erkennbar sind, die ein Hochladen der Ancestry-Daten z. B. bei Gedmatch verhindern würden. Richtig ist weiterhin, dass über ein solches Hochladen Verwandte einem Risiko, in Strafverfolgungsmaßnahmen einbezogen zu werden, ausgesetzt werden. Richtig ist weiterhin, dass Ancestry auf dieses Risiko nicht hinweist. Richtig ist schließlich, dass Strafverfolgungsbehörden gemäß dem jeweils anwendbaren Strafverfolgungsrecht (insbesondere der USA) auf den Datenbestand von Ancestry zugreifen können und dass damit ein Strafverfolgungsrisiko bei biologisch Verwandten begründet oder erhöht wird.

Punkt 10: Es trifft zu, dass das Gendiagnostikgesetz (GenDG) bei Forschungszwecken nicht zu einer humangenetischen Beratung verpflichtet. Mein Gutachten stellt aber dar, dass die Voraussetzungen für eine Forschungsprivilegierung bei den Auswertungen durch Ancestry nicht vorliegen, wozu u. a. Transparenz, Nachprüfbarkeit, Kritikoffenheit gehören (BVerfGE 35, 112f.). Vom GenDG wird eine humangenetische Beratung nicht nur bei diagnostischen und prädiktiven Gentest gefordert, auch für die „Klärung der Abstammung" wird eine umfassende Aufklärung gefordert. Ancestry ergreift – soweit erkennbar – keine wirksamen Maßnahmen um zu verhindern, dass die bereitgestellten Rohdaten für diese Zwecke verwendet werden.

Punkt 11: Meine Behauptung, dass Ancestry nicht die Berechtigung zur Einsendung der Speichelproben prüft, wird nicht dadurch widerlegt, dass in den Nutzungsbedingungen eine missbräuchliche Einsendung verboten wird. Tatsächlich erfolgt keine wirksame Identitäts- geschweige denn Berechtigungsprüfung durch Ancestry. Die Behauptung, es läge nicht in der Verantwortung von Ancestry, dass sich die Nutzungsbedingungen „im Einzelfall umgehen lassen", ist falsch. Gemäß der Rechtsprechung des Europäischen Gerichtshofs (U. v. 5.6.2018 – C-210/16) besteht bei Ancestry für den Umgang mit den Gendaten zumindest eine „gemeinsame Verantwortlichkeit". Dies bedingt, dass Ancestry dann auch notwendige und angemessene Schutzvorkehrungen treffen muss. Derartige Maßnahmen sind nicht zu erkennen (Art. 26, 24 DSGVO).

Punkt 12: Zwar untersagt Ancestry die Verwendung der DNA-Analyse für einen „Vaterschaftstest", doch klärt das Unternehmen nicht über die Folgen eines solchen, technisch einfach durchzuführenden Tests (Strafbarkeit, Verletzung des Rechts auf Nichtwissen, familiäre Verwerfungen, psychische Schäden) auf, der für den Einsendenden zudem nur mit einem minimalen Überführungsrisiko verbunden ist. Es ist geradezu eine Verharmlosung, wenn die Kenntniserlangung „über unerwartete Fakten zu Ihrer ethnischen Zugehörigkeit" als (negative) Folge benannt wird.

Thilo Weichert 12.06.2019

URL der Erwiderung:
https://digitalcourage.de/blog/2019/erwiderung-bigbrotherawards-ancestry

Eine mit einer Fristsetzung verbundene Aufforderung, einige ehrverletzende Falschdarstellungen in der Internet-Veröffentlichung zu unterlassen, führte dazu, dass der Autor Tobias A. Kemper seinen Text kurzfristig änderte und die offensichtlich rechtswidrigen Aussagen korrigierte. Seitdem findet eine Debatte über die genetischen Genealogie-Angebote in Deutschland statt. Alle Versuche, mit den Kreisen in der Geneaologie-Szene ins direkte Gespräch zu kommen, die derartige Online-Angebote gut finden, sind bisher gescheitert. Auch die Versuche des Netzwerks Datenschutzexpertise wie auch von DigitalCourage, Ancestry zu einem Dialog zu bringen, blieben ohne inhaltliche Resonanz.

Eine interessante Reaktion zeigte die Bild-Zeitung: Direkt nach der Veröffentlichung des Saecula-Blogs von Herrn Kemper wurde das BBA-Team von einem Bild-Journalisten aufgefordert, innerhalb von knapp zwei Tagen dazu Stellung zu nehmen. Dies führte dann zu der ausführlichen Reaktion des BBA-Jury-Mitglieds Thilo Weichert, die dieser der Bild-Zeitung zur Verfügung stellte, verbunden mit der Aufforderung, darüber ausführlich zu berichten. Aus dem Bericht wurde nichts, auch nachdem der anfragende Bild-Journalist nochmals eindringlich aufgefordert worden war, über dieses die Bild-Zeitung-Lesenden

sicher stark interessierende Thema zu berichten. Recherchen ergaben dann, dass „Bild" bei dem Thema nicht gerade neutral ist und es deshalb wohl auch mit der journalistischen Sorgfalts- und Berichtspflicht nicht so ernst nimmt: Bild führte nämlich zum offiziellen Markteintritt von AncestryDNA in Deutschland ein Gewinnspiel durch mit dem Titel „Mit ancestry.de die eigene Familie entdecken", bei dem „zwei Sets bestehend aus einem AncestryDNA-Test, einer Halbjahres-Mitgliedschaft für ancestry.de sowie einem Notebook von Dell" exklusiv verlost wurden. Es ging dabei darum, einfach eine Gewinnspielanfrage zu beantworten. Teilnahmeschluss war 23:55 am 02.12.2018.

https://www.bild.de/partner/unterhaltung/gewinnspiele/adventskalender-02_ancestry-58658320.bild.html

Am 04.01.2019 hatte der später anfragende Bild-Journalist begeistert über seine „Familienforschung mit dem Wattestäbchen" berichtet.

https://www.bild.de/bild-plus/digital/internet/internet/erbgut-analyse-was-verraet-ein-dna-test-ueber-meine-vorfahren-59298722,view=conversionToLogin.bild.html

Das Thema liegt inzwischen beim zuständigen Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) sowie beim Verbraucherzentrale Bundesverband (vzbv). Beide können tätig werden. Das BayLDA ist aber dazu solange nicht verpflichtet, solange nicht ein direkt Betroffener eine Beschwerde einreicht. Der vzbv könnte eine Unterlassungserklärung einfordern und bei zu erwartender Verweigerung durch Ancestry eine Verbandsklage einreichen. Das Problem ist aber, dass weder beim BayLDA noch beim vzbv derzeit Ressourcen für ein Vorgehen gegen Ancestry – oder auch gegen andere Anbieter, die sich an den deutschen Markt wenden, wie z. B. MyHeritage – vorhanden sind.

Aufgegriffen wurde das Thema von Gen-ethischen Netzwerk, die hierzu schon einige Aktivitäten gestartet haben.

https://www.gen-ethisches-netzwerk.de/gene-und-genome/gentests-und-genomsequenzierung

Am 02.07.2019 hielt Isabelle Bartram von Gen-ethischen Netzwerk auf dem 83. Netzpolitischen Abend der Digitalen Gesellschaft in Berlin dazu einen Vortrag, der im Internet abrufbar ist:

https://youtu.be/3UZupEUlhMM

Die Auseinandersetzung zu dem Thema steht also erst ganz am Anfang. Die DANA wird hierüber weiter berichten.

Zivilgesellschaftliche Organisationen fordern die korrekte Bewertung der Vorratsdatenspeicherung

Übersetzung: Markus Eßfeld und Frank Spaeing

In Vorbereitung einer möglichen Gesetzgebung führt die EU-Kommission mit diversen Interessenvertretungen derzeit einen Dialog. Es geht dabei um die Erörterung von Möglichkeiten zur Umsetzung von Vorratsdatenspeicherung gemäß der Vorgaben des Europäischen Gerichtshofs (EuGH) und des Europäischen Gerichtshofs für Menschenrechte (EGMR). EDRi hat sich im Rahmen des erwähnten Dialogs am 06.06.2019 mit der Generaldirektion der EU-Kommission für Migration und Inneres getroffen.

Am 22.07.2019 haben 30 zivilgesellschaftliche Organisationen einen offenen Brief an die designierte EU-Kommissionspräsidentin Ursula von der Leyen und die EU-Kommissare Avramopoulos (Migration, Inneres und Bürgerschaft), Jourová (Justiz, Verbraucherschutz und Gleichstellung) sowie King (Sicherheitsunion) gesandt. Gefordert wird eine unabhängige Bewertung der Notwendigkeit und Verhältnismäßigkeit bereits bestehender und künftig zu erwartender Gesetzgebung zum Thema Vorratsdatenspeicherung. Ferner haben die Unterzeichnenden darum gebeten sicherzustellen, dass die Diskussion um die Vorratsdatenspeicherung keine Verzögerung des Inkrafttretens der ePrivacy-Verordnung herbeiführt.

Offener Brief des Vereins European Digital Rights[1 2 3] vom 22.07.2019 an die Europäische Kommission[4]

Die Verfasser dieses Briefes repräsentieren Nichtregierungsorganisationen (NGO), die daran arbeiten Menschenrechte im virtuellen bzw. digitalen Raum zu schützen und zu fördern. Dieser Brief dient insbesondere dem Ziel Vorschläge zu unterbreiten zur Sicherstellung der Compliance mit der EU-Grundrechtscharta und der dazugehörenden Rechtsprechung des Europäischen Gerichtshofs (EuGH), soweit es um das Recht zur Vorratsdatenspeicherung geht.

Am 08.04.2014 hat der EuGH die Richtlinie 2006/24/EG über die Vorratsspeicherung für ungültig erklärt. Das Urteil selbst wird von verschiedenen Mitgliedsstaaten der EU (und Ländern des europäischen Wirtschaftsraumes) unterschiedlich interpretiert. Der Verein European Digital Rights (EDRi) hat in einer Studie herausgefunden, dass sechs Mitgliedsstaaten[5] ihre Vorratsdatenspeicherung nach wie vor auf eine Weise regeln, die dem EuGH-Urteil widerspricht. Andere Erhebungen wiesen in dieselbe Richtung[6]. Obwohl die Daten von Millionen Europäern weiterhin illegal gespeichert wurden, hatte die Europäische Kommission kein Vertragsverletzungsverfahren eingeleitet.

Im Nachgang zum EuGH-Urteil über die Vorratsdatenspeicherung im Fall Tele2 ./. Watson vom 21.12.2016 hat der Juristische Dienst des EUGH in eindeutiger Weise erklärt, dass „eine generelle und willkürliche [wahllose] Vorratsdatenspeicherung mit dem Ziel der Verbrechensverhütung und anderer Sicherheitsgründe auf nationalstaatlicher Ebene nicht anders geregelt werden darf als auf europäischer Ebene. Denn eine solche – nationalstaatliche – Regelung würde grundlegende Anforderungen verletzen, wie sie vom EuGH in zwei jüngsten Entscheidungen[7] von der Großen Kammer formuliert worden sind“.[8]

Am 06.06.2019 hat der Europäische Rat[9] „Schlussfolgerungen im Hinblick auf die zukünftige Entwicklung der Vorratsdatenspeicherung mit dem Ziel der Verbrechensbekämpfung“ verabschiedet. Diese Schlussfolgerungen beschreiben „die Vorratsdatenspeicherung als wesentliches Mittel, um gegen schwere Straftaten effizient ermitteln zu können“. Der Europäische Rat bittet die EU-Kommission, „weitere Informationen zu sammeln und gezielte Befragungen durchzuführen, um in einer Studie die denkbaren Lösungen für eine Vorratsdatenspeicherung darzustellen“. Eingeschlossen sind ausdrücklich Gesetzgebungsinitiativen zum Thema.

Während die ungeprüfte und umfassende Vorratsdatenspeicherung insbesondere für Strafverfolgungsbehörden von hohem Interesse ist, wurde nie bewiesen, dass die willkürliche Speicherung von Positions- und Metadaten von über 500 Millionen Europäern notwendig, verhältnismäßig oder überhaupt nur wirkungsvoll sei.

Die ungeprüfte und umfassende Vorratsdatenspeicherung ist ein die Privatsphäre erheblich verletzender Überwachungsakt, der sich gegen die gesamte Bevölkerung der EU richtet. Zur Folge hat eine solche Vorratsdatenspeicherung ggf. die Speicherung vertraulicher Informationen über soziale Kontakte (einschließlich solcher geschäftlicher Art), Bewegungen innerhalb Europas sowie Informationen aus dem Privatleben (Kontakte zu Ärzten, Rechtsanwälten, Arbeitnehmervertretungen, Psychologen, Hilfs- und Beratungsstellen u.a.) von hunderten von Millionen Europäern – und das in Abwesenheit eines begründeten Verdachts für die Vorratsdatenspeicherung, also anlasslos.

Die Vorratsdatenspeicherung von Telekommunikationsdaten unterminiert die gesetzlich garantierte Schweigepflicht der beratenden Berufe und schreckt die Bürger ab, vertrauliche Informationen auf elektronischem Wege zu teilen. Außerdem ist die Vorratsdatenspeicherung von hohem Interesse für die organisierte Kriminalität und für illegal eingreifende staatliche Akteure. Zahlreiche Datenschutzverletzungen sind in der Vergangenheit dokumentiert worden[10]. Die allgemeine Vorratsdatenspeicherung erschüttert im weiteren den Schutz journalistischer Quellen und damit die Freiheit der Presse. Mithin geht es hier um die Beschädigung von wesentlichen Grundlagen offener und freiheitlicher Gesellschaften.

Die unterzeichnenden Organisationen dieses Offenen Briefes haben daher den konstruktiven Dialog mit der Europäischen Kommission gesucht. Dabei ging es insbesondere darum, bei den „zukünftigen Entwicklungen“ die folgenden maßgeblichen Vorschläge zu beachten:

- die Europäische Kommission möge eine unabhängige wissenschaftliche Studie über die Notwendigkeit und Verhältnismäßigkeit bisheriger und potentiell geplanter gesetzgeberischer Maßnahmen zum Thema Vorratsdatenspeicherung in Auftrag geben, dabei beachtend die Frage der Menschenrechte und der Aufklärungsquote bei Verbrechen;
- die Europäische Kommission und der Europäische Rat mögen sicherstellen, dass die neu entfachte Debatte über Vorratsdatenspeicherung die rasche Annahme der ePrivacy-Verordnung nicht verhindert,
- die Europäische Kommission möge bei der Europäischen Agentur für Grundrechte (FRALEX) eine rechtsvergleichende Studie in Auftrag geben mit dem Ziel der Darstellung aller derzeit existierenden Gesetze zur Vorratsdatenspeicherung und ihrer Compliance mit der EU-Grundrechtscharta und allen einschlägigen Entscheidungen des Europäischen Gerichtshofs sowie des Europäischen Gerichtshofs für Menschenrechte zur Vorratsdatenspeicherung.
- die Europäische Kommission möge Vertragsverletzungsverfahren gegen die Mitgliedsstaaten der EU durchführen, deren Vorratsdatenspeicherungsgesetze gegen geltendes europäisches Recht verstoßen.

Wir sehen der Antwort der Kommission entgegen und stehen zu Ihrer Verfügung, um notwendige gesetzliche Initiativen zu unterstützen, die dem EU-Recht auf diesem wichtigen Rechtsgebiet Geltung verschaffen werden.

Es folgen zahlreiche NGO, die den offenen Brief unterschrieben haben[11].

1 Internationaler gemeinnütziger Verein nach belgischem Recht

2 Im Folgenden: EDRi

3 EDRi plus 29 mitzeichnende NGO

4 Im englischen Original sind diverse Kommissionsmitglieder als Adressaten namentlich aufgeführt

5 https://edri.org/edri-asks-european-commission-investigate-illegal-data-retention-laws/

6 Nachzulesen beispielsweise bei: Privacy International, 2017, National Data Retention Laws since Tele-2/Watson Judgement: https://www.privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf

7 Gemeint sind die hier bereits erwähnten Urteile des EuGH

8 Council document 5884/17, paragraph 13

9 Gem. Art. 15 II EUV: Staats- und Regierungschefs der Mitgliedsstaaten, Präsident der Kommission, u.a.

10 Ein aktuelles Beispiel wäre dies: https://techcrunch.com/2019/06/24/hackers-cell-networks-call-records-theft/

11 Siehe dazu den im Original nachfolgend abgedruckten Brief

22 July 2019

By email:
President-elect von der Leyen
First Vice-President Timmermans

CC:
Commissioner Avramopoulos
Commissioner Jourová
Commissioner King

Dear President-elect von der Leyen,
Dear First Vice-President Timmermans,

The undersigned organisations represent non-governmental organisations working to protect and promote human rights in digital and connected spaces. We are writing to put forward suggestions to ensure compliance with the EU Charter of Fundamental Rights and the CJEU case law on data retention.

EU Member States (and EEA countries) have had different degrees of implementation of the CJEU ruling on 8 April 2014 invalidating the Data Retention Directive. EDRi's 2015 study reported that six Member States[1] have kept data retention laws which contained features that are similar or identical to those that were ruled to be contrary to the EU Charter. Other evidence pointed in the same direction.[2] While personal data of millions of Europeans were being stored illegally, the European Commission had not launched any infringement procedures. On 21 December 2016, the CJEU delivered its judgment in the Tele2/Watson case regarding data retention in Member States' national law. In the aftermath of this judgment, the Council Legal Service unambiguously concluded that "a general and indiscriminate retention obligation for crime prevention and other security reasons would no more be possible at national level than it is at EU level, since it would violate just as much the fundamental requirements as demonstrated by the Court's insistence in two judgments delivered in Grand Chamber."[3]

On 6 June 2019 the Council adopted "conclusions on the way forward with regard to the retention of electronic communication data for the purpose of fighting crime" which claim that "data retention is an essential tool for investigating serious crime efficiently". The Council tasked the Commission to "gather further information and organise targeted consultations as part of a comprehensive study on possible solutions for retaining data, including the consideration of a future legislative initiative."

1 https://edri.org/edri-asks-european-commission-investigate-illegal-data-retention-laws/
2 See, for example. Privacy International, 2017, *National Data Retention Laws since Tele-2/Watson Judgment*: https://www.privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf
3 Council document 5884/17, paragraph 13

While the concept of blanket data retention appeals to law enforcement agencies, it has never been shown that the indiscriminate retention of traffic and location data of over 500 million Europeans was necessary, proportionate or even effective.

Blanket data retention is an invasive surveillance measure of the entire population. This can entail the collection of sensitive information about social contacts (including business contacts), movements and private lives (e.g. contacts with physicians, lawyers, workers councils, psychologists, helplines, etc.) of hundreds of millions of Europeans, in the absence of any suspicion. Telecommunications data retention undermines professional confidentiality and deters citizens from making confidential communications via electronic communication networks. The retained data is also of high interest for criminal organisations and unauthorised state actors from all over the world. Several successful data breaches have been documented.[4] Blanket data retention also undermines the protection of journalistic sources and thus compromises the freedom of the press. Overall, it damages preconditions of open and democratic societies.

The undersigned organisations have therefore been in constructive dialogue with the European Commission services to ensure that the way forward includes the following suggestions: :

- The European Commission commissions an independent, scientific study on the necessity and proportionality of existing and potential legislative measures around data retention, including a human rights impact assessment and a comparison of crime clearance rates;
- The European Commission and the Council ensure that the debate around data retention does not prevent the ePrivacy Regulation from being adopted swiftly;
- The European Commission tasks the EU Fundamental Rights Agency (FRA) to prepare a comprehensive study on all existing data retention legislation and their compliance with the Charter and the CJEU/European Court of Human Rights case law on this matter;
- The European Commission consider launching infringement procedures against Member States that enforce illegal data retention laws.

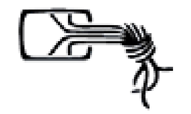
We look forward to your response and remain at your disposal to support the necessary initiatives to uphold EU law in this policy area.

4 A recent example can be found here: https://techcrunch.com/2019/06/24/hackers-cell-networks-call-records-theft/

Signatories:















dataskydd.net

Digital Rights Ireland



















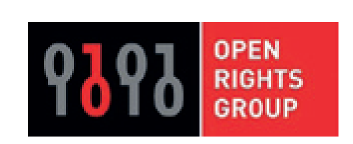
























Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Kirchentag fordert „Sicherheit und Vertrauen in der digitalen Gesellschaft"

Das größte Treffen von ChristInnen in Deutschland, der vom 19. bis zum 23.06.2019 in Düsseldorf stattfindende Deutsche Evangelische Kirchentag, verabschiedete eine Resolution gegen Überwachung der Menschen durch Unternehmen und Staaten. Diese kritisiert die aktuelle Digitalpolitik der Bundesregierung und spricht sich für mehr Verschlüsselung, mehr Datenschutz und die Einhaltung von Grundrechten aus. Sie fordert ein offizielles Recht auf Verschlüsselung und ein Ende der Ausnutzung von Sicherheitslücken durch staatliche Stellen sowie ein klares Bekenntnis zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die von netzpolitik.org vorgeschlagene Resolution mit dem Titel „Sicherheit und Vertrauen in der digitalen Gesellschaft" wurde mit 600 Ja-Stimmen bei 6 Gegenstimmen und 15 Enthaltungen angenommen. So kritisiert die unter anderem an Bundeskanzlerin Merkel und Bundesinnenminister Seehofer gerichtete Resolution die zunehmende Überwachung von Menschen durch Unternehmen und Staaten. Auch Deutschland wird für die beispiellose Ausweitung staatlicher Befugnisse und für Gesetze kritisiert, denen es an Verhältnismäßigkeit und Augenmaß fehle.

Der Leitspruch der evangelischen Großveranstaltung lautete „Was für ein Vertrauen" – eine Steilvorlage für eine Auseinandersetzung mit dem Problem der IT-Sicherheit. Obwohl das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme heute wichtiger denn je sei, werde es gemäß der Resolution bisher nicht mit Leben gefüllt. Das liege auch an der widersprüchlichen Politik der Bundesregierung, die Sicherheit für alle garantieren soll, deren Behörden gleichzeitig aber Sicherheitslücken horten, um sie für Überwachung zu nutzen. Erst wenige Wochen zuvor hatte Innenminister Horst Seehofer Hintertüren zu jeglicher verschlüsselter Privatkommunikation und Zugang zu Daten aus digitalen Assistenzsystemen gefordert. Die Resolution hält dem entgegen, dass nur diejenigen sich frei informieren, bilden und entwickeln können, die sich sicher sein können, nicht permanent beobachtet zu werden. Der Text betont die Wichtigkeit vertraulicher Kommunikation für freien und unabhängigen Journalismus. Sichere Kommunikation schütze elementare Bestandteile der Demokratie.

Die Resolution fordert weiterhin, dass Deutschland zum Verschlüsselungsstandort Nr. 1 werden müsse, was ein Recht auf Verschlüsselung beinhalte. Außerdem sollten IT-Sicherheitslücken nicht von staatlichen Stellen ausgenutzt werden, was ein Bekenntnis des Kirchentages gegen die Einführung und Nutzung von Staatstrojanern darstellt. Weitere Forderungen sind die Förderung von quelloffenen und datenschutzfreundlichen Kommunikations- und Sicherheitslösungen, der Ausbau des Datenschutzes durch eine personelle Stärkung der Datenschutzbehörden sowie ein massiver Ausbau von Förderprogrammen in Sachen Digitalkompetenzen für alle Teile der Gesellschaft (Reuter, Kirchentag an Bundesregierung: Schützt die Vertraulichkeit der Kommunikation!, netzpolitik.org 22.06.2019).

Bund

Regierung: Smarthome-Abhören kein „Lauschangriff"

Gemäß einer Antwort der Bundesregierung auf eine kleine Anfrage der FDP-Fraktion ist ein Zugriff der Sicherheitsbehörden auf Daten von Smarthome-Geräten ohne eine gesetzliche Neuregelung möglich. Das Bundesinnenministerium führt aus, dass es sich bei den Geräten nicht „um eine neue Geräteklasse handele, die vom bestehenden Rechtsrahmen nicht umfasst sei". Der Bundesdatenschutzbeauftragte (BfDI) Ulrich Kelber sieht das anders. Er sprach in diesem Zusammenhang unlängst von einer „verfassungsrechtlich bedenklichen Kompetenzerweiterung".

Unter Smarthome-Geräten versteht man etwa den Amazon-Lautsprecher Echo mit dem Sprachassistenten Alexa, aber auch Luftsensoren, Bewegungsmelder oder Überwachungskameras, die Informationen versenden. Gemäß der Antwort ist die Bundesregierung der Ansicht, dass für den Zugriff auf vernetzte Geräte nicht die Voraussetzungen gelten, die für die Anordnung einer akustischen Wohnraumüberwachung - den sogenannten großen Lauschangriff - notwendig sind. Vielmehr kämen die weniger hohen Hürden für die Online-Durchsuchung zur Anwendung. Darunter versteht man den Eingriff in einen Computer oder ein anderes informationstechnisches System ohne Wissen des Betroffenen. Zwar ist in beiden Fällen ein richterlicher Beschluss notwendig, und es muss sich um Ermittlungen zu einer besonders schweren Straftat handeln. Bei der akustischen Überwachung kommt jedoch noch hinzu, dass es Anhaltspunkte geben muss, „dass durch die Überwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind". Der FDP-Innenpolitiker Benjamin Strasser wies darauf hin, dass grundsätzlich „alle digitalen und vernetzten Geräte mit Mikrofon" für die akustische Überwachung genutzt werden können. Für die Bundesregierung biete dies „ein millionenfaches Potenzial für Wanzen

im Wohnzimmer" („Wanzen im Wohnzimmer", SZ 15.07.2019, 5).

Bund

Elektronische Patientenakte kommt ohne differenzierten Zugriff

Von Januar 2021 an soll die elektronische Patientenakte (ePA) für alle PatientInnen in Deutschland zur Verfügung stehen. Doch wird es am Anfang nicht möglich sein auszuwählen, welche ihrer persönlichen Informationen ein Arzt, Apotheker oder Therapeut einsehen darf und welche nicht. Der Grund ist die angeblich von Bundesgesundheitsminister Jens Spahn (CDU) für die Einführung der Akte gesetzte zu kurze Frist. Ein Physiotherapeut, der Einblick in die elektronischen Daten des Orthopäden braucht, wird auf diese Weise zum Beispiel auch über einen Schwangerschaftsabbruch seiner Patientin informiert. Ein Apotheker erfährt automatisch auch von der Psychotherapie seines Kunden. Aus Sicht der gesundheitspolitischen Sprecherin der Grünen, Maria Klein-Schmeink, ist dies ein echtes Problem für die Akzeptanz der elektronischen Akte in der Bevölkerung und unter den ÄrztInnen.

Will eine PatientIn also in Zukunft ihre elektronische Akte nutzen und zum Beispiel vermeiden, dass ihr Zahnarzt die Informationen des Urologen lesen kann, hat sie zwei Möglichkeiten: Entweder, sie verbietet dem Urologen, ihr Untersuchungsergebnis in die Akte zu schicken – dann kann später niemand diese Unterlagen nutzen, auch nicht das Krankenhaus oder der Hausarzt. Oder sie verbietet dem Zahnarzt den Zugriff auf die Akte. Über frühere Behandlungen erfährt er dann aber auch nichts. Übrig bliebe nur noch ein Bereich in der elektronischen Akte, in dem PatientInnen zum Beispiel Artikel aus der „Apothekenumschau" speichern oder Daten aus einer Gesundheitsapp unterbringen können, womit ÄrztInnen im Zweifel nicht viel anfangen können.

Die Gesellschaft für Telematikanwendungen der Gesundheitskarte (Gematik), die für die Entwicklung der Akte verantwortlich ist, erklärte, eine „differenzierte Rechtevergabe soll in Folgestufen umgesetzt werden". Wann genau PatientInnen die elektronische Akte individuell einstellen können und nicht jedem Gesundheitsdienstleister, der die Akte nutzen soll, auch gleich ihren HIV-Test oder ihr Depressionstagebuch präsentieren müssen, sollen nun die Gesellschafter der Gematik entscheiden. Seit Mitte Mai 2019 gehört zu diesen Gesellschaftern auch das Bundesgesundheitsministerium mit einem Anteil von 51%.

Vertreter der Gematik erklärten gegenüber Bundestagsabgeordneten, der Grund für die technischen Abstriche sei die kurze Frist gewesen, die der Bundesgesundheitsminister gesetzt habe. Aufgrund dieses Zeitdrucks habe man sich entschieden, die Patientenakte Anfang 2021 erst einmal einzuführen und dann die Rechte für PatientInnen nachzuliefern. Die elektronische Patientenakte ist von der Bundesregierung seit knapp 15 Jahren beschlossen und geplant. Spahn hatte sich vorgenommen, sie in seiner Amtszeit endlich einzuführen (Ludwig, Datenschutz wird nachgeliefert, SZ 21.05.2019, 6; www.sueddeutsche.de 21.05.2019).

Bund

Stasi-Überprüfung verlängert

30 Jahre nach dem Fall der Mauer sollten die Stasi-Überprüfungen bei Mitarbeitern im öffentlichen Dienst auslaufen. Die Bundesregierung will sie nun verlängern – ebenso wie die Entschädigungen für Opfer des SED-Regimes. Gemäß einem Gesetzentwurf zur Änderung des Stasi-Unterlagengesetzes, der am 15.05.2019 beschlossen worden ist, sollen leitende Mitarbeiter im öffentlichen Dienst auch im kommenden Jahrzehnt auf eine frühere hauptamtliche oder inoffizielle Tätigkeit für die DDR-Staatssicherheit hin überprüft werden. Die Verlängerung bis 2030 war im Koalitionsvertrag vereinbart worden. Kulturstaatsministerin Monika Grütters (CDU) erklärte: „Nicht zuletzt aus Respekt vor den Opfern der SED-Diktatur ist eine Überprüfung möglicher informeller Mitarbeiter weiterhin notwendig und wichtig." Im Jahr 2018 gab es 167 Anträge auf Stasi-Überprüfung im öffentlichen Dienst und 446 Anträge auf Überprüfung von Mandatsträgern. Die Vorsitzende des Kulturausschusses, die SPD-Politikerin Katrin Budde, meinte auch, die Fristverlängerung sei richtig. Menschen, die wie sie selbst 54 Jahre alt seien, könnten durchaus noch für die Stasi gearbeitet haben und sich jetzt erstmals für den öffentlichen Dienst bewerben. Deshalb müssten sie überprüft werden. „Im Jahr 2030 wird es derartige Fälle kaum noch geben."

Zudem sollen Opfer des SED-Regimes über das Jahr 2020 hinaus entschädigt werden. Ein Entwurf der damaligen Justizministerin Katarina Barley (SPD) sieht zudem vor, dass die Entschädigung für Heimkinder erleichtert und erweitert wird. Nach derzeitiger Rechtslage würden die SED-Unrechtsbereinigungsgesetze in diesem und im kommenden Jahr auslaufen. Sie regeln die Rehabilitierung und Entschädigung für Opfer der SED-Willkürherrschaft. Für Kinder, deren Eltern verfolgt wurden und die selbst keinen Anspruch auf Rehabilitierung haben, soll damit ein neuer Anspruch auf Unterstützungsleistungen geschaffen werden (Wehner, Stasi-Überprüfung geht weiter, www.faz.net 14.05.2019; Stasi-Überprüfung verlängert, SZ 16.05.2019, 5)

Bund

Handballspieler werden gläsern

Die Handball-Bundesliga (HBL) führt zur Saison 2019/2020 eine Technologie ein, die diesen Sport attraktiver machen soll. Mittels eines Chips, der in den Trikots der Spieler sowie in einer Blase im Inneren des Balls integriert ist, werden umfassend Daten erfasst und analysiert, wodurch erkannt werden kann, welcher Spieler am schnellsten und am meisten läuft, wer am höchsten springt oder am härtesten wirft. Neben Teams und Trainern sollen auch Fans und Medien von den Erkenntnissen profitieren. Durch 14 Wlan-Router pro Arena werden die Daten in Sekundenbruchteilen zusammengefügt und abrufbar gemacht. Frank Bohmann, Geschäftsführer der HBL, verspricht eine „neue Erlebniswelt" mit „faszinierenden Blickwinkeln". Maik Machulla, Trainer des deutschen Meisters SG Flensburg-

Handewitt, erläutert: „Durch das Tracking haben wir im Wettkampf und Training einen kontinuierlichen Einblick in die Leistungsparameter jedes Spielers. So kann die Verfügbarkeit zusätzlicher Daten die Früherkennung unterstützen und Spieler vor Verletzungen schützen."

Die HBL arbeitet mit dem Münchner Unternehmen Kinexon zusammen, das mittels der integrierten Chips die Daten erfasst, analysiert und in Echtzeit aufbereitet. In den amerikanischen Profiligen NBA (Basketball) und NFL (American Football) nutzen bereits einige Klubs die Technologie im Training, um Leistungswerte zu ermitteln. Die deutschen Handballer sind die ersten, die diese Möglichkeiten nicht nur ihren Klubs und Trainern zur Verfügung stellen wollen, sondern auch der Öffentlichkeit, vor allem Medien und Fans.

Liga-Chef Bohmann glaubt, „dass diese Art der Datenerfassung für jede medial aufbereitete Sportart in mittelfristiger Zukunft Standard sein wird". Fernsehsender sollen die Daten in ihre Live-Übertragungen einfließen lassen; Fans sollen sie über eine App abrufen können. Mit der hübschen Spielerei können sie während einer laufenden Partie sofort sehen, wer sich am meisten reinhängt, wer am kräftigsten wirft, wer am meisten rennt. So solle vor allem ein junges Publikum angesprochen werden.

Unternehmen und Liga versichern, dass alle Datenschutzrichtlinien eingehalten würden. Erkennbar sind nicht nur die Spieler mit höchsten Leistungsscores, sondern auch die, die z. B. bei einer Niederlage am wenigsten gerannt sind und am schwächsten geworfen haben. So lässt sich Fan-Unmut auf eine Zielscheibe kanalisieren. Zudem besteht das Risiko, dass ZuschauerInnen nur noch aufs Smartphone blicken und aus den Augen verlieren, was sich in der analogen Realität abspielt (Chip im Trikot, Mölter, Gläserne Spieler, glänzende Zukunft, SZ 08.05.2019, 25).

Bund

Fälschungssichere Kassensysteme gefordert

Die Finanzministerin von Schleswig-Holstein Monika Heinold (Grüne) und der Hamburger Finanzsenator Andreas Dressel (SPD) haben den Bundesfinanzminister Olaf Scholz (SPD) in einem gemeinsamen Brief aufgefordert, entschlossener gegen den Milliardenbetrug durch Manipulation von Kassen in Geschäften oder Gaststätten vorzugehen. Der Bundestag hat zwar ein Gesetz beschlossen, nach dem bis Anfang 2010 rund zwei Millionen Kassen mit einer zertifizierten technischen Sicherheitseinrichtung (TSE) ausgestattet sein müssen. Doch räumte das Finanzministerium intern ein, dass die notwendige Technik noch nicht fertig entwickelt ist. Heinold und Dressel fordern nun als Alternative, das mithilfe des Bundes entwickelte sogenannte Insika-Verfahren zu nutzen, das bislang nur in Taxametern zum Einsatz kommt. Die beiden MinisterInnen verweisen auf Österreich, wo 2017 ein Insika-nahes Verfahren eingeführt wurde. Dort habe der Staat schon im ersten Jahr 650 Mio. Euro Umsatzsteuern zusätzlich eingenommen. Dressel erklärte: „Für den wahrscheinlichen Fall einer verzögerten Einführung von TSE brauchen wir dringend einen Plan B." Heinold appellierte an den Bund, „endlich im Interesse der Steuergerechtigkeit zu handeln" (Taxameter als Vorbild, Der Spiegel Nr. 20, 11.05.2019, S. 23)

Bundesweit

Lidl personalisiert Werbung

Der Discounter Lidl nutzt als erster Lebensmittelhändler in Deutschland in großem Stil Big Data in seinen Märkten. Die sogenannte digitale Lidl-Kundenkarte gibt es schon in mehreren europäischen Ländern, darunter Österreich, Nordspanien, Polen und Dänemark. Vom 14.06.2019 an können auch die KundInnen in den etwa 250 Lidl-Filialen in Berlin und Brandenburg die Smartphone-App namens Lidl Plus nutzen. Nach einer Testphase soll die App dann 2020 in ganz Deutschland freigeschaltet werden. Mithilfe der App will Lidl das Einkaufsverhalten der KundInnen im Detail auswerten. In einer Pressemitteilung wirbt Dominik Eberhard, der Geschäftsführer Digital bei Lidl Deutschland, mit den vermeintlichen Vorteilen für die KundInnen dank dieser Software: „Mit der neuen digitalen Kundenkarte bieten wir den Lidl-Fans die Möglichkeit, bei jedem Einkauf bares Geld zu sparen."

Die App ermöglicht es, einzelnen KundInnen aufgrund der Analyse ihres Kaufverhaltens personalisierte Angebote zu machen. Individuelle, auf das Smartphone gespielte Rabattcoupons werden dabei den jeweiligen Personen offeriert. Die Packung Müsli, das Viererpack Joghurt oder die Tüte Süßigkeiten eines bestimmten Herstellers hat in dem Moment nicht mehr für alle den gleichen Preis, sondern wird individuell angepasst. Ob das zur Kundenzufriedenheit führt, ist umstritten.

Coupons sind zwar nichts Neues in Deutschland, neu hingegen sind die Big-Data-Auswertung des Kaufverhaltens und die damit verbundenen personenspezifischen Angebote. Der Discounter verhehlt nicht seine Absicht, die Umsätze zu steigern. Für das Herunterladen der App erhält die KundIn einen „Fünf-Euro-Willkommenscoupon". Den kann sie einlösen, wenn sie für mindestens 25 Euro einkauft, was relativ viel für einen „Durchschnittsbon" bei dem Discounter ist. Die personalisierten Angebote beschränken sich nicht nur auf Produkte, die in den Lidl-Märkten erhältlich sind. Sie können auch bei Partnern eingelöst werden, wie etwa bei Flixbus und anderen regionalen Partnern, die in der App sichtbar werden.

Obwohl die Software erst 2020 bundesweit ausgerollt werden soll, sind die dafür nötigen Scanner bereits an allen deutschen Lidl-Kassen aufgebaut. Die Daten werden nicht nur im Laden generiert, Lidl identifiziert die KundInnen auch, wenn sie online einkaufen. Onlinehändler wie Amazon werten die Daten der KundInnen heute schon auf ähnliche Weise aus. Auch überwiegend stationäre Händler wie der Modeanbieter Zara tun dies. Onlinehändler sind gegenüber stationären Händlern in der Regel im Vorteil, was die Datenauswertung betrifft. Gerade den Lebensmittelhändlern sind die Daten ihrer KundInnen bisher weitgehend unbekannt geblieben, obwohl diese in der Regel oft wiederkehren. Lidl will nun diesen „Nachteil" ausgleichen. Die Genehmigung zur Auswertung der Daten holt sich der Discounter auf seinen Webse-

ten, in der App oder im Newsletter. Lidl lässt sich auch genehmigen, über die Geolokalisierung des Handys ortsbezogene Werbung zu senden und Angebote am „bevorzugten Einkaufstag" zu verschicken. Die KundInnen müssen entscheiden, ob sie das wollen (Kläsgen, Big Data im Discounter, SZ 12.06.2019, 17).

Bundesweit

Apple-Kamerawagen erfassen Straßen und Häuser

Neun Jahre nach dem Streit über Google Street View schickt jetzt Apple Kamerawagen durch Deutschland, um die Aufnahmen für Apple Maps zu nutzen und damit das neue Angebot „Look Around" zu realisieren. Die mit Spezialkameras bestückten 80 Autos sind in deutschen Städten seit dem 29.07.2019 bis ca. Mitte September auf den Straßen unterwegs und erstellen Aufnahmen von Straßen und Gebäuden. Laut Apple sollen die Daten in erster Linie das Kartenmaterial verbessern. Die Bilder werden voraussichtlich auch in dem neuen Panorama-Dienst Look Around zum Einsatz kommen - Apples Konkurrenzangebot zu Google Street View, das kurz zuvor im Juni auf der Entwicklerkonferenz WWDC angekündigt worden war. Apple informiert auf einer Website, in welchen Gegenden die Fahrzeuge eingesetzt sind.

Vor ihrem Einsatz in Deutschland waren die Kamerawagen innerhalb Europas bereits in Großbritannien, Frankreich, Italien, Spanien, Portugal, Kroatien und Slowenien unterwegs. Vor dem Start der Fahrten in Deutschland war Apple mit dem bayerischen Landesamt für Datenschutzaufsicht in Kontakt. Die Daten aus den Fahrzeugen werden auf Apples Server in den USA geladen. Bei Look Around können Nutzende sich auf dem Bildschirm durch dreidimensionale Darstellungen von Straßenzügen bewegen. Die Funktion soll im Herbst zunächst für einige ausgewählte Gebiete in den USA verfügbar werden, darunter die Umgebung von San Francisco, in der viele Apple-Mitarbeitende zu Hause sind.

Vor einer möglichen Einführung dieses Angebots in Deutschland - und direkt zum Start der Kamerawagen-Fahrten - bietet Apple Nutzenden die Möglichkeit an, die Löschung (Verpixelung) von Rohdaten mit Abbildungen von Personen oder Häusern zu beantragen. Die entsprechende Seite soll im Laufe des Dienstags live geschaltet werden. Gesichter und Autokennzeichen werden bei Look Around - wie auch bei Googles Street View - automatisch verpixelt. Laut Apple erreichte die dafür verwendete Software bei Tests mit Fotodaten aus der Umgebung von San Francisco eine Trefferquote von fast hundert Prozent. Apple kann aus den von seinen Fahrzeugen erfassten Bilddaten unter anderem Informationen wie Straßennamen, die Namen von Geschäften sowie Daten zu Verkehrszeichen und Straßenführung extrahieren. Zusätzlich zu den Kameras sind die Fahrzeuge mit Laser-Radaren ausgestattet, die ihre Umgebung dreidimensional abtasten. Die auch unter dem Namen Lidar bekannten Geräte werden unter anderem in selbstfahrenden Autos eingesetzt.

Per GPS zeichnen die Fahrzeuge während der Fahrt zudem Ortsdaten auf, sodass alle unterwegs aufgezeichneten Informationen später exakten Positionen auf der Karte zugeordnet werden können. Andere Daten werden laut Apple nicht erhoben. Bei Google hatten die Kamera-Fahrzeuge seinerzeit zur präziseren Orientierung auch die Kennungen und Signalstärken von WLANs registriert, speicherten aber auch Fragmente unverschlüsselter WLAN-Übertragungen. Das war vom Hamburger Datenschutzbeauftragten Johannes Caspar aufgedeckt und beanstandet worden; Google sprach damals von einem Fehler (Street-View-Konkurrent Look Around Apples Kameraautos sollen deutsche Straßen fotografieren, www.spiegel.de 23.07.2019; Apple schaut sich um, SZ 24.07.2019, 19).

Baden-Württemberg

Getsafe schlussfolgert aus Online-Verhalten auf Risiko

Wenn das Versicherungs-Start-up Getsafe aus Heidelberg mit einer KundIn online einen Vertrag über eine Hausratversicherung abschließt, dann kommt es nicht nur auf Wohnort, Größe der Wohnung oder Wert der Möbel an. Mitbegründer und Firmenchef Christian Wiens erläutert: „Wir schauen uns an, wie lange jemand auf unserer Seite braucht, um einen Vertrag abzuschließen." Wer länger als zwölf Minuten benötigt, habe im Schnitt weniger Schäden. Wer sich in weniger als sechs Minuten durchklickt, stelle ein höheres Risiko dar. Dies kann sich im Preis oder bei der Beurteilung von Schäden niederschlagen.

Getsafe vermisst mit Methoden der künstlichen Intelligenz die KundInnen. Vier Jahre nach der Gründung steht die Firma vor einem Wachstumsschub. Sie hat sich gerade bei Investoren unter Führung der Berliner Firma Earlybird 15 Mio. Euro gesichert und so die Finanzierung auf 21 Mio. Euro gebracht. Getsafe hatte im Frühsommer 2019 ca. 60.000 Policen, wobei gemäß Wiens etwa die Hälfte davon über das Vergleichsportal Check24 kam. Bis Ende 2019 will das Start-up den Bestand auf 180.000 Verträge steigern. Die Mitarbeiterzahl wollen Wiens und Mitgründer Marius Blaesing von 55 auf 100 steigern. Noch 2019 geht Getsafe nach Großbritannien: „Italien, Frankreich und Spanien folgen 2020." Getsafe verkauft bisher eine Haftpflicht- und Hausratspolice mit Fahrradversicherung, eine Zahnzusatzpolice und Rechtsschutz. „2020 wollen wir auch Risikolebens- und Berufsunfähigkeitspolicen anbieten." Getsafe arbeitet als Assekuradeur, übernimmt also Risikobeurteilung, Verwaltung und Schadenbearbeitung, trägt aber nicht das Risiko. Das macht die Munich Re. Die KundInnen sind im Schnitt 29 Jahre alt, 75% hatten vorher noch keine Versicherung. Wiens ist selbstbewusst: „Wir sind die Nummer eins bei den Versicherungseinsteigern" (Fromme, Die Kunden vermessen, SZ 07.06.2019, 26).

Baden-Württemberg

DSGVO-Bußgeld gegen Polizisten

Der baden-württembergische Landesdatenschutzbeauftragte Stefan Brink hat nach Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) und

des neuen Landesdatenschutzgesetzes (LDSG) sein erstes Bußgeld gegen einen Mitarbeiter einer öffentlichen Stelle verhängt. Der mittlerweile rechtskräftige Bußgeldbescheid in Höhe von 1.400 Euro richtet sich gegen einen Polizeibeamten, der dienstlich erlangte personenbezogene Daten unzulässig eigenmächtig für private Zwecke weiterverarbeitete.

Der Polizist fragte ohne dienstlichen Bezug mithilfe seiner Nutzerkennung über das Zentrale Verkehrsinformationssystem (ZEVIS) des Kraftfahrbundesamtes (KBA) die Halterdaten für ein Kfz-Kennzeichen einer privaten Zufallsbekanntschaft ab. Mit den so gewonnenen Personalien habe er im Anschluss eine automatisierte Abfrage bei der Bundesnetzagentur durchgeführt, über die er neben den Personendaten der Geschädigten auch die dort hinterlegten Festnetz- und Mobilfunknummern in die Finger bekam. Ohne dienstlichen Grund und ohne das Plazet der Betroffenen habe er daraufhin telefonisch Kontakt mit dieser aufgenommen.

Zwar ist eine Ahndung von Datenschutzverstößen gegenüber öffentlichen Stellen gemäß dem LDSG Baden-Württemberg nicht vorgesehen. Da das Fehlverhalten nicht der Dienststelle zurechenbar und der Täter auch nicht als „eigene öffentliche Stelle" agierte, war ein Bußgeld möglich. Die Höhe des Bußgeldes ist nach Ansicht von Brink angemessen, da es „sich um einen Erstverstoß handelte, bei dem nur eine Person betroffen war" (Krempl, DSGVO: Datenschutzaufsicht im Ländle verhängt erstes Bußgeld gegen Polizeibeamten, www.heise.de 18.06.2019, Kurzlink: https://heise.de/-4450131).

Bayern

Kfz-Kennzeichenscanning zur Verdachtsgewinnung

Die bayerische Polizei hat nach Angaben des dortigen Innenministeriums im Jahr 2018 in sieben Fällen mit Kfz-Kennzeichen-Scannern nach Autos gesucht, um eine Datengrundlage für weitere Ermittlungen zu erlangen. In den ersten 4 Monaten des Jahres 2019 geschah dies offenbar schon dreimal. Üblicherweise darf mit dem Kfz-Kennzeichen-Scanning auf Straßen nur nach Nummernschildern in Fahndungslisten gesucht werden, also wenn ein konkreter Straftatverdacht schon bestätigt ist. In den genannten Fällen war es dagegen darum gegangen, „erst Ermittlungsansätze" zu gewinnen. Die Kennzeichen wurden erfasst, um sie im Rahmen weiterer Ermittlungsschritte und Datenabgleiche weiter auszuwerten. Patrick Breyer von der Piratenpartei kritisiert: „Anders als immer wieder beteuert, werden also nicht gesuchte Kennzeichen nicht gleich wieder gelöscht." Die Scanner würden „zur lückenlosen Autofahrer-Erfassung zweckentfremdet" (Fotos auf Vorrat, Der Spiegel Nr. 20, 11.05.2019 S. 23).

Bayern

Radar-Körperscanner für Stadionbesuchende geplant

Ein neues Sicherheitssystem soll den Einlass ins Fußballstadion des FC Bayern München in Fröttmaning künftig schneller und einfacher machen. Von der Jahresmitte 2020 an will das Technologieunternehmen Liberty Defense, dessen Zentrale im kanadischen Toronto liegt, bei Heimspielen einen neuartigen Körperscanner testen. Der „Hexwave"-Scanner soll bei den BesucherInnen im Vorbeigehen nach Waffen und Pyrotechnik suchen, ohne dass diese etwas davon spüren. Dies soll mit Hilfe von Radarstrahlen erfolgen. Der FC Bayern und Liberty Defense wollen durch den Einsatz der Technologie künftig Menschenschlangen beim Einlass vermeiden. Unternehmenssprecherin Brittany Whitmore betonte: „Die Strahlung, die wir dabei verwenden, ist ausgesprochen niedrig". Sie habe eine ähnliche Frequenz wie handelsübliche Wlan-Strahlung, sei jedoch etwa 200 Mal geringer. Trotzdem könne Hexwave Textilien durchleuchten. Die Strahlung werde von festen Materialien, die sich unter der Kleidung befänden, reflektiert, so entstehe ein digitales Abbild des Trägers. Dieses Abbild prüfe dann eine Künstliche Intelligenz auf Anomalien, die ein verbotener Gegenstand sein könnten: „Wenn das System eine solche Anomalie entdeckt, verständigt es automatisch das Sicherheitsteam im Stadion."

Der FC Bayern erhofft sich durch die Zusammenarbeit mit Hexwave eine weitere Erhöhung des Sicherheitsstandards sowie eine Erleichterung des Stadionzutritts. Liberty Defense seinerseits verspricht sich von der Kooperation Praxisdaten, aus denen ihr System lernen kann. Hexwave entwickelt sich mithilfe von sogenannten Deep-Learning-Prozessen selbst weiter und soll so mit jeder Person, die es kontrolliert, besser darin werden, versteckte Gegenstände zu entdecken. Die Erprobung vor der Münchner Arena ist also für den Hersteller wichtig, um das System marktreif zu machen, so Whitmore: „Für den FC Bayern wird das System daher auch nichts kosten." Da es sich lediglich um einen Test handelt, wird gemäß der Unternehmenssprecherin das neue Sicherheitssystem voraussichtlich nicht sofort an allen Eingängen des Stadions eingesetzt werden: „Wo und in welchem Umfang Hexwave in München zum Einsatz kommt, müssen unsere Techniker erst mit den Sicherheitsexperten vor Ort abklären." Diesen Punkt hätten Liberty Defense und der FC Bayern in ihrer gemeinsamen Planung noch nicht erreicht. StadionbesucherInnen müssen sich also auch 2020 noch auf die klassischen Taschenkontrollen durch das Sicherheitspersonal einstellen.

Die Münchner Arena ist bisher europaweit der einzige Standort, an dem ein Beta-Test für das neue System vorgesehen ist. Weltweit wird es weitere Tests geben. Im April 2019 unterzeichnete Liberty Defense ähnliche Absichtserklärungen mit dem Betreiber der Rogers Arena im kanadischen Vancouver, der Heimstätte der Eishockeymannschaft Canucks, sowie mit dem US-amerikanischen Kaufhausinvestor Sleiman Enterprises. Im Mai 2019 folgte eine gemeinsame Erklärung mit dem Generalstaatsanwalt des Bundesstaats Utah, Sean Reyes (Republikaner), um den Körperscanner in öffentlichen Gebäuden des Bundesstaats sowie bei Veranstaltungen zu erproben. In Utah löste das eine öffentliche Debatte aus. Bürgerrechtsorganisationen werfen dem Generalstaatsanwalt und Liberty Defense vor, die EinwohnerInnen Utahs als Versuchskaninchen für

eine unausgereifte Technologie missbrauchen zu wollen. Falsch identifizierte medizinische Geräte wie Insulinpumpen oder Herzschrittmacher könnten für ihre Träger zu unnötigen Befragungen durch die Sicherheitsbehörden führen. Außerdem ebne die Einführung derartiger Systeme den Weg in den Überwachungsstaat. Eingriffe in die Privatsphäre würden normalisiert, was aus Sicht der Bürgerrechtsorganisationen ein Verstoß gegen die amerikanische Verfassung ist. Liberty Defense erwiderte, Hexwave sei weitaus weniger invasiv als bereits gängige Systeme wie z. B. die umstrittene automatische Gesichtserkennung. Whitmore: „Die Bilder werden lediglich von der Künstlichen Intelligenz ausgewertet und sofort wieder gelöscht, wenn sie keine Auffälligkeiten bemerkt." Es würden keinerlei personenbezogene Daten durch die Software gespeichert. Deutsche Datenschützer müssten aus diesem Grund auch keine Angst vor Hexwave haben (Wolfeger, Körperscanner beim FCB, SZ 24.06.2019, 28).

Niedersachsen

Polizei- und Ordnungsgesetz verabschiedet

Am 14.05.2019 hat der Niedersächsische Landtag mit den Stimmen von SPD und CDU ein neues Polizei- und Ordnungsbehördengesetz mit zusätzlichen Befugnissen zur Datenverarbeitung beschlossen. Innenminister Boris Pistorius (SPD) begrüßte die Verabschiedung, mit der den Sicherheitskräften mehr Möglichkeiten bei der Terrorismusbekämpfung zugestanden würden: „Es ist unverzichtbar, dass wir gerade in Sicherheitsfragen immer auf der Höhe der Zeit bleiben." Das alte Polizeigesetz stamme noch aus dem Jahr 2007, dem Jahr, in dem das erste Smartphone auf den Markt gekommen sei. Am Wochenende vor dem Parlamentsbeschluss waren noch einmal viele Menschen gegen die Verschärfungen auf die Straße gegangen.

Vor der Beschlussfassung hatten umfangreiche Ausschussberatungen stattgefunden, in denen der Regierungsentwurf mehrheitlich von den GutachterInnen als europa- und verfassungswidrig kritisiert worden war. Kritik äußerten u. a. das Netzwerk Datenschutzexpertise sowie die Landesbeauftragte Barbara Thiel. Die Kritik hatte zur Folge, dass einige Regelungen überarbeitet wurden. So darf das neue Überwachungsinstrument der sog. elektronischen Fußfessel nur von einem Richter angeordnet werden, was zunächst nicht geplant war. Gleiches gilt für Aufenthaltsvorgaben, Kontaktverbote oder für längerfristige Meldeauflagen. Für die Videoüberwachung im öffentlichen Raum sind erstmals Höchstspeicherfristen vorgesehen. Bildmaterial darf im Regelfall sechs Wochen gespeichert werden. Es wurden datenschutzrechtliche Verfahrensvorschriften verankert, die eine wirksame Datenschutzkontrolle ermöglichen sollen. So sind u. a. heimlich durchgeführte polizeiliche Maßnahmen besonders zu begründen und zu dokumentieren. Die Kontrollmöglichkeiten des Parlaments gegenüber der Polizei bei besonders grundrechtsrelevanten Eingriffsbefugnissen wurden ausgeweitet.

Die maximale Dauer einer Präventivhaft wurde zwar gegenüber dem Erstentwurf halbiert, ist aber gegenüber dem vorherigen Rechtszustand immer noch massiv auf 35 Tage ausgeweitet worden. Das neue Gefahrenabwehrrecht enthält nunmehr einen rechtlichen Rahmen für den Einsatz von Bodycams. Die Videoüberwachung zur Verkehrsüberwachung und für die streckenbezogene Geschwindigkeitskontrolle (Section Control) wurde geregelt, was die Datenschutzbeauftragte Thiel begrüßte: „Die mit diesen Maßnahmen verbundene Datenverarbeitung wurde bisher von der Polizei ohne ausreichende Rechtsgrundlage durchgeführt. Dieser verfassungswidrige Zustand wird nunmehr beseitigt." Die Rechtswidrigkeit dieses Vorgehens war erst mit Beschluss vom 10.05.2019 vom Oberverwaltungsgericht Lüneburg bestätigt worden (Az. 12 ME 68/19; zur 1. Instanz DANA 2019, 110). Fraglich bleibe, ob das Land für diese Form der Geschwindigkeitsmessung überhaupt eine Gesetzgebungskompetenz besitze.

Dennoch vertritt Thiel die Ansicht, dass das neue Gesetz an vielen Stellen weiterhin verfassungswidrig und deshalb korrekturbedürftig ist. So wurden die Eingriffsschwellen für viele polizeiliche Maßnahmen ohne stichhaltige Begründung herabgesetzt. Online-Durchsuchungen oder die elektronische Fußfessel können schon im Vorfeld einer konkreten Gefahrenlage angeordnet werden. Die Befugnisse zur Quellen-Telekommunikationsüberwachung und zur Online-Durchsuchung unter Einsatz so genannter Staatstrojaner sind für Thiel als unverhältnismäßige Grundrechtseingriffe nicht akzeptabel. Staatliche Behörden müssten bewusst Sicherheitslücken in der IT offenhalten, um Staatstrojaner einsetzen zu können. Dies widerspräche der staatlichen Pflicht, die IT-Infrastruktur umfassend vor Cyberangriffen zu schützen. Die Opposition aus Grünen und FDP kündigte an, gegen das Gesetz gerichtlich vorzugehen und sucht Mitstreiter im Landtag für eine Normenkontrollklage beim Staatsgerichtshof.

Die Landesbeauftragte kritisierte zudem die fehlende Umsetzung der seit dem 06.05.2018 geltenden europäischen Datenschutzrichtlinie für Justiz und Inneres: „Damit werden die Daten von Bürgerinnen und Bürgern im Bereich der Gefahrenabwehr und Straftatenverhütung nach wie vor europarechtswidrig verarbeitet." Die Koalitionsfraktionen und das Innenministerium kündigten insofern eine weitere Gesetzesnovellierung an (Die Landesbeauftragte für den Datenschutz Niedersachsen, PE 14.05.2019, Datenschutz verbessert, aber immer noch europa-rechtswidrig; Polizeigesetz verabschiedet, SZ 15.05.2019, 5; Krempl, Niedersachsen: Polizei darf künftig Trojaner und Streckenradar einsetzen, www.heise.de 14.05.2019; Stellungnahme des Netzwerks Datenschutzexpertise zum Regierungsentwurf https://www.netzwerk-datenschutzexpertise.de/sites/default/files/br_2018_npog.pdf).

Nordrhein-Westfalen

AZR-Abfrage durch BA-Mitarbeiter verängstigt ägyptischen Flüchtling

Das Nachrichtenmagazin Fakt berichtete am 21.05.2019 in der ARD über einen bemerkenswerten Fall des Missbrauchs des Ausländerzentralregisters

(AZR), das unter der Aufsicht des Bundesinnenministeriums vom Bundesamt für Migration und Flüchtlinge (BAMF) betrieben wird. Auf die dort gespeicherten umfassenden Daten über AusländerInnen, die sich länger als 3 Monate in Deutschland aufhalten, also auch über Flüchtlinge, haben viele Stellen in Deutschland Zugriff, von Sicherheitsbehörden bis hin zu Sozialbehörden. Im Jahr 2018 erfolgten durchschnittlich pro Tag 190.000 Datenabrufe. Durch das im Frühjahr 2019 verabschiedete sog. 2. Datenaustauschverbesserungsgesetz wurde die Kontrolle diese Abrufe erschwert.

Omar Ismail ist ein Asylsuchender aus Alexandria/Ägypten, der sich im 2. Ausbildungsjahr als Altenpfleger in Deutschland befindet. Sein Name soll auf einer Todesliste gestanden haben. Er geriet zwischen die Fronten der Auseinandersetzung zwischen der Muslimbrüderschaft und der ägyptischen Regierung. Sein Bruder war verhaftet worden und kam während der Haft zu Tode. Ismail informierte über seinen Facebook-Account auf Arabisch, wie man über das Fachkräfteeinwanderungsgesetz legal nach Deutschland kommen kann. Daraufhin erhielt er über Facebook eine Nachricht, in der ihm mitgeteilt wurde, er solle bei Flüchtlingen keine falsche Hoffnungen auslösen. Zur Bekräftigung seines Post und als Nachweis, dass er ein „Beamter" und damit ein „Big Boss" sei, sandte der Absender einen AZR-Auszug von Ismail mit höchstpersönlichen Informationen. Dieser bekam es – nicht zu Unrecht – mit der Angst zu tun, dass nun seine ägyptischen Verfolger Zugriff auf seine Daten und ihn möglicherweise auch in Deutschland im Visier hätten, und zog deshalb aus seiner Wohnung aus. Er erstattete Anzeige bei den Strafverfolgungsbehörden in Herford wegen des illegalen Abrufens und Nutzens von AZR-Daten und legte das Chatprotokoll vor. Die Staatsanwaltschaft stellte das Verfahren ein, weil der Täter nicht ermittelt werden könnte, so die Mitteilung. Dem Journalistenteam von Fakt fiel es dagegen leicht, den Urheber des Posts anhand seines Facebook-Accounts zu identifizieren. Der Landsmann von Ismail bot über Facebook seine Dienste unter dem Namen Mido M. als Reisebegleiter in Arabisch an. Es handelte sich um einen Sachbearbeiter bei der Bundesagentur für Arbeit (BA), der dann auch dem Journalisten treuherzig bestätigte, dass er die Daten beim AZR abgerufen hatte. Konfrontiert mit diesen journalistischen Erkenntnissen antwortete die Staatsanwaltschaft Bielefeld, sie habe offenbar die vorhandenen Ermittlungsansätze zunächst nicht „vollständig gewürdigt".

Datenschutznachrichten aus dem Ausland

Weltweit

Google transkribiert Aufnahmen von Sprachassistenten

Nachdem Entsprechendes schon zu Amazons Alexa (Echo) bekannt wurde, zeigt sich nun, dass auch Google Audio-Aufnahmen seines Sprachassistenten von Mitarbeitenden von Vertragsunternehmen teilweise begutachten und mitschreiben lässt. Dem belgischen Rundfunksender VRT wurden von einem Whistleblower über 1.000 solcher Mitschnitte zugespielt. Die Aufnahmen hätten es in einigen Fällen ermöglicht, die betroffenen NutzerInnen dahinter ausfindig zu machen. Einer der Informanten ist gemäß dem Bericht bei einer Vertragsfirma angestellt; weltweit soll es mehrere tausend Personen geben, die solche von Google-Home-Lautsprechern und der Google-Assistant-App angelegten Audioschnipsel bearbeiten. In Flandern und den Niederlanden seien es rund ein Dutzend Mitarbeitende, die sich um Aufnahmen in Niederländisch kümmern. Damit soll die Spracherkennung des Systems verbessert werden.

Zum Einsatz komme dabei das auch frei zugängliche Crowdsourcing-Werkzeug Crowdsource. Die Funktionen für die Beschreibung von Audioschnipseln seien Mitarbeitenden vorbehalten. Diese sollten dann die Mitschnitte so akkurat wie möglich beschreiben, etwa mit Details wie dem Geschlecht der Sprechenden. Auch solle alles Hörbare inklusive Elementen wie etwa Hustern protokolliert werden. Eigentlich soll die Sprachassistenz erst durch eine Aktivierung etwa durch Fingertipp oder mit dem Aufwachbefehl „Ok, Google" aktiv werden und aufzeichnen. Offenbar ist aber auch Googles System für Fehlerkennungen anfällig. Der Rundfunksender berichtet, dass 153 der etwas über 1.000 Aufnahmen wohl nicht hätten aufgezeichnet werden sollen. Unter anderem seien es private Konversationen etwa zwischen Eltern und Kindern gewesen, Streits oder berufliche Telefongespräche, die so aufgenommen wurden.

Eine der Quellen berichtete von einer Aufnahme, bei der eine Frau offensichtlich in Not gewesen sei. Für solche Fälle gäbe es aber keine Richtlinien von Google, was die Mitarbeitenden tun sollten. Lediglich wenn es etwa um Account-Daten, Passwörter und ähnliches ginge, sollten diese als sensitiv gekennzeichnet werden. Bei vielen der an die Assistenten gerichteten Fragen ginge es um medizinische Dinge, bei Männern sei auch die Suche nach Pornographie verbreitet. Schon im April 2019 wurde mit ganz ähnlichen Details berichtet, wie Mitarbeitende von Vertragsunternehmens von Amazon weltweit Tonaufnahmen von Alexa transkribieren (DANA 2/2019, 95 f.). Google hatte damals erklärt, wie man mit Assistant-Aufnahmen umgeht: „Bei Google können einige Mitarbeiter auf einige Audioausschnitte aus dem Assistant zugreifen, um das Produkt zu trainieren und zu verbessern. Diese sind aber nicht mit persönlich identifizierbaren Informationen verknüpft und die Audiosequenzen sind verzerrt." Gemäß den nun vorgelegten Berichten sind dagegen die Aufnahmen der Google-Home-Spre-

chenden sehr klar gewesen, die Aufnahmen über die Smartphone-App Google Assistant hätten zumindest Telefonqualität gehabt. Ton-Verzerrungen habe es keine gegeben. Google gab dazu keine Stellungnahme ab.

Gemäß dem Bericht werden bei den Aufnahmen für die Bearbeitung Namen und Accountinformationen entfernt und durch Sequenznummern ersetzt. Doch genüge aufmerksames Zuhören teilweise, um die Sprechenden zu identifizieren. So seien Adressen und andere sensitive Informationen gut zu hören gewesen. Im Zuge der Berichterstattung recherchierte der berichtende Rundfunksender VRT einige der identifizierbaren Personen und konfrontierte sie mit den Aufnahmen. Ein Mann habe sofort seine Stimme erkannt, ein älteres Ehepaar die Stimmen von Sohn und Enkel. Google erklärte, dass man weltweit mit SprachexpertInnen zusammenarbeite, um die Sprachassistenz besser zu machen. Dafür werde eine kleine Zahl von Audiodateien transkribiert und analysiert, rund 0,2% aller Aufnahmen. Absolute Zahlen nannte Google nicht. Dieses Vorgehen sei entscheidend für die Entwicklung von Technologien, die Produkte wie den Google Assistant unterstützen. Eine Verknüpfung zu persönlich identifizierbaren Informationen gebe es nicht. Und: „Wir haben erfahren, dass einer dieser Prüfer gegen unsere Datenschutzrichtlinien verstoßen hat, indem er vertrauliche Audiodaten aus den Niederlanden weitergegeben hat. Unsere Sicherheits- und Datenschutzteams sind involviert und ermitteln bereits. Wir werden entsprechende Maßnahmen ergreifen und eine umfassende Überprüfung der Sicherheitsvorkehrungen durchführen, um zu verhindern, dass sich so etwas wiederholt“ (Kannenberg, Googles Sprachassistent: Mitarbeiter hören und bewerten Audioaufnahmen, www.heise.de 11.07.2019, Kurzlink: https://heise.de/-4467985).

EU

Europäischer Datenschutz-Berufsverband EFDPO gegründet

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. ist Initiator eines europäischen Dachverbands der Datenschutzbeauftragten, der sich am 07.06.2019 in Berlin gegründet hat. Gründungsmitglieder der European Federation of Data Protection Officers (EFDPO) sind neben dem BvD nationale Verbände für Datenschutzbeauftragte aus Österreich, Frankreich, Portugal, Tschechien, der Slowakei, Griechenland und Liechtenstein. Hauptziel der Gründung ist es, die Datenschutzbeauftragten der EU-Mitgliedsstaaten miteinander zu vernetzen, gemeinsame Standards zu entwickeln und die Interessen in Brüssel zu vertreten. Dabei soll Datenschutz als Wettbewerbs- und Standortvorteil für Europa gestärkt werden. Arbeitssitz des neuen Verbandes ist Brüssel. EFDPO will sich unter anderem auch dafür einsetzen, einen EU-weiten Zertifizierungsstandard für Datenschutzbeauftragte zu etablieren.

BvD-Vorstandsvorsitzender Thomas Spaeing: „Betriebliche Datenschutzbeauftragte sind wichtige Akteure zur Einhaltung datenschutzrechtlicher Bestimmungen. Als Datenschutzexperten stellen sie die unternehmerische Handlungsfähigkeit unter der DSGVO sicher und sorgen zugleich dafür, dass die Verbraucher- und Bürgerrechte beim Datenschutz eingehalten werden. Das entlastet auch die nationalen Datenschutz-Aufsichtsbehörden.“ Wie der BvD e.V. ist auch der neue Dachverband nicht auf Datenschutzbeauftragte beschränkt, sondern berücksichtigt auch die Interessen weiterer im Bereich Datenschutz entstehender Berufe wie den Datenschutzauditor oder den Datenschutzkoordinator. In einigen EU-Länder wie Portugal oder Tschechien werden erste Erfahrungen mit betrieblichen Datenschutzbeauftragten gemacht.

Gründungsmitglieder der EFDPO sind: Deutschland: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. www.bvdnet.de, APDPO PORTUGAL Associação dos Profissionais de Proteção e de Segurança de Dados (Portugal), Spolek pro ochranu osobních údajů (Czech Republic), Spolok na ochranu osobných údajov (Slovakia), Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter privacyofficers.at. (Austria), UDPO, Union des DPO's (France), dsv.li-Datenschutzverein in Liechtenstein (Liechtenstein), HADPP – Helenic Association of dpp (Greece).

Ansprechpartner: BvD Pressestelle, Tel: 030 26 36 77 60, Budapester Straße 31, 10787 Berlin, E-Mail: pressestelle@bvdnet.de, Internet: https://www.bvdnet.de (Eggert, Neugründung EU-Dachverband für Datenschutzbeauftragte, www.bvdnet.de 11.06.2019)

EU

Digitale Fahrgastkontrolle bei Schiff, Bus und Bahn?

Es herrscht Streit zwischen den EU-Mitgliedstaaten, ob Reisende in Bussen, Zügen und Schiffen schärfer überwacht und detaillierte Datensätze über ihre Fahrten angelegt werden sollen. Dies ergibt sich aus der Zusammenfassung eines Treffens der zuständigen Arbeitsgruppe des EU-Rates vom 03.07.2019 in der ständigen Vertretung Deutschlands bei der EU. Einen solchen sogenannten Passenger Name Record (PNR) erheben derzeit Fluglinien über ihre Passagiere. Erfasst werden unter anderem Name, Adresse, Buchungscode, Reiseverlauf sowie Informationen über die Bezahlung, den Vielflieger-Status, den Sitzplatz und das Gepäck. Die Fluglinien leiten die Informationen an Sicherheitsbehörden weiter, in Deutschland an das Bundeskriminalamt (BKA). In der Arbeitsgruppe „Informationsaustausch“ des EU-Rates geht es jetzt um die Frage, ob die Praxis auch auf den See- und Landweg ausgeweitet werden soll. Die meisten Staaten unterstützen die Idee, sehen aber juristische und praktische Hindernisse.

Die europäische PNR-Richtlinie gilt seit Sommer 2018. In Deutschland nehmen bislang 25 Luftfahrtunternehmen teil. Ist das System voll im Einsatz, dürfte es im Jahr mehr als 200 Millionen Menschen erfassen, die in Deutschland starten und landen. BürgerrechtlerInnen sehen in der Maßnahme eine unzulässige anlasslose Massenüberwachung. Die Gesellschaft für Freiheitsrechte hat Klagen gegen das BKA und zwei Fluglinien eingereicht. Elisabeth Niekrenz von der Nichtregierungsorganisation Digita-

le Gesellschaft warnt: „Würde auch der Schiffs- und Bahnverkehr erfasst, käme das einer vollständigen Überwachung der europäischen Reisebewegungen nahe – völlig unverhältnismäßig."

Die Zusammenfassung des Arbeitsgruppen-Treffens zeigt, dass mehrere Staaten das Verfahren im Namen des Kampfes gegen Terrorismus und Organisierte Kriminalität ausdehnen wollen. Teilnehmende verwiesen auf das Phänomen des „broken travel" – des „unterbrochenen Reisens". Ihnen zufolge wechselten Terroristen oft die Verkehrsmittel, reisten etwa erst per Flugzeug, dann per Bus oder Bahn. Das spreche für die Ausweitung von PNR. Auch ein deutscher Vertreter verwies auf dieses „Phänomen". Belgien fordert seit Jahren, auch Zugreisende zu erfassen. Dort werden dem Bericht zufolge in Pilotprojekten bereits Daten über KundInnen von Flixbus und Eurostar-Zügen erfasst.

Der Vertreter Deutschlands verhielt sich dem Bericht zufolge „weisungsgemäß ablehnend". Er habe darauf verwiesen, dass der Grundrechtseingriff durch PNR so „intensiviert" werde. Das Bundesinnenministerium erklärt auf Anfrage, man habe sich zur Ausweitung von PNR „noch keine Position gebildet". Wie die Überwachung von Bus-, Schiff- und Zugreisenden praktisch umgesetzt werden könnte, ist derweil unklar. Deutschland wandte ein, man solle erst die Auswertung des PNR-Systems für Flüge 2020 abwarten. Zudem seien „Bahntickets in Deutschland nicht zwangsläufig personengebunden, und die Flexibilität sei ein wesentlicher Vorteil der Eisenbahn in Deutschland". Es fehle auch ein einheitliches Datenformat wie bei den Fluggastdaten. Auch Belgien als Verfechter einer Ausweitung gab zu bedenken, die Daten seien „heterogen". Das mache es schwierig, Daten verschiedener Verkehrsmittel auszuwerten und abzugleichen.

Anhand der Daten über Flugpassagiere, die schon erhoben werden, sollen Algorithmen bald Verdächtige schon vor einer Tat identifizieren. So könnte zum Beispiel eine Kombination aus einer bestimmten Reiseroute, etwa in Nahost, und der Barzahlung von Tickets einen Alarm auslösen, der dann an menschliche Ermittler weitergeleitet wird. Gegen diese Form der Datensammlung wendet sich Moritz Körner, Mitglied der FDP-Fraktion im Europäischen Parlament: „Die Ausdehnung der anlasslosen Reiseüberwachung reduziert den privaten Bewegungsradius der Menschen weiter." 99,7% der vermeintlichen PNR-Treffer seien Irrtümer gewesen. „Statt mehr Datenmüll brauchen wir endlich mehr Kooperation zwischen den Ermittlungsbehörden. Wir werden die Nadel im Heuhaufen nicht schneller finden, indem wir den Heuhaufen größer und größer machen." Die neue Bundesjustizministerin Christine Lambrecht (SPD) warnte davor, Profile von Passagieren aus Bahn-, Fernbus- und Schiffsreisen verpflichtend automatisiert an die Polizei weiterzuleiten. Das wäre „ein erheblich weitergehender Eingriff in Grundrechte als nur die Speicherung von Fluggastdaten: Hier gerät das Verhältnis von Freiheit und Sicherheit ins Wanken." Es könnten Bewegungsprofile entstehen, auch von völlig unverdächtigen BürgerInnen. „Das Gefühl, dass der Staat weiß, wann ich wohin reise, kann zu gravierenden Einschränkungen der persönlichen Freiheit führen." Sie lobte das derzeitige Buchungssystem der Bahn: „Es ist ein großer Wert, dass wir flexibel reisen können, meist ohne Zugbindung und ohne namensgebundene Tickets. Eine Speicherung der Ticketdaten wäre damit gar nicht möglich." SZ-Kommentator Jannis Brühl: „Die Ausweitung von PNR wäre ein Verrat an einer der besten Ideen Europas: der Reisefreiheit. Denn wie frei ist eine Reise, wenn der Staat jede Buchung registriert und analysiert?" Bis Ende Juli 2019 reichen die Staaten schriftlich ihre Kommentare in der Gruppe ein (Brühl, Digitale Fahrgastkontrolle, SZ 17.07.2019, 7; ders. im Netz gefangen, SZ 17.07.2019, 4; ders. Reisen ohne Bewegungsprofil, SZ 19.07.2019, 7; vgl. DANA 1/2018, 44).

EU

Butarelli gestorben

Der Europäische Datenschutzbeauftragte Giovanni Buttarelli ist am 20.08.2019 im Kreise seiner Familie verstorben. Er litt seit längerem unter gesundheitlichen Problemen. Der Europäische Datenschutzbeauftragte ist die unabhängige Kontrollinstanz für die EU-Institutionen. Der im Alter von 62 verstorbene Buttarelli war seit 2014 als Datenschutzbeauftragter für die Einhaltung des Datenschutzes durch die EU-Institutionen zuständig und ist gemeinsam mit Vertretern der nationalen Behörden Mitglied des Europäischen Datenschutzausschusses. Vor seiner Amtszeit war Buttarelli in seinem Heimatland Italien Richter und Generalsekretär der Datenschutzbehörde, außerdem war er als Experte für den Europarat und die OSZE tätig.

In Buttarellis Amtszeit erhielt der Schutz der Privatsphäre durch das Inkrafttreten der Datenschutzgrundverordnung und Skandale wie jenen um Cambridge Analytica globales Gewicht. Der italienische Jurist nutzte das Amt des EU-Datenschutzbeauftragten, um öffentlich auf strenge Einhaltung der Regeln durch Staaten und globale Konzerne zu pochen. Buttarelli hat sein Amt gestärkt und für den Datenschutz in Europa wichtige Schritte gesetzt. Als Datenschutzbeauftragter könnte ihm nun sein bisheriger Stellvertreter Wojciech Wiewiórowski nachfolgen. Der Nachfolger oder die Nachfolgerin wird in einer gemeinsamen Entscheidung des Europäischen Parlaments und des Rates der Mitgliedsstaaten ernannt (Fanta, Europäischer Datenschutzbeauftragter Giovanni Buttarelli verstorben, netzpolitik.org, 21.08.2019)

Schweiz

Datenschutzmaterialien für 4- bis 9-Jährige vorgestellt

Der kantonale Datenschutzbeauftragte und die Pädagogische Hochschule Zürich haben Unterrichtsmaterialien für 4- bis 9-jährige Kinder entwickelt, die diese befähigen sollen, kompetent mit ihren Daten umzugehen, und haben sie anlässlich des 13. Europäischen Datenschutztags am 28.01.2019 vorgestellt: Welches Geheimnis kann ich für mich behalten, und welches sollte ich besser einem Erwachsenen anvertrauen? Was gebe ich anderen Menschen mit bestimmten Informationen über mich preis? Je früher Kinder diese Fragen beantworten können, desto besser sind sie für das digitale Zeitalter gerüstet. Die Kinder sollen lernen, warum Privat-

sphäre wichtig ist und wie sie ihre Daten schützen können.

Das Lehrmittel heißt „Geheimnisse sind erlaubt“. Es handelt sich um ein E-Book mit fünf Unterrichtseinheiten. Kindergartenkinder werden mithilfe eines dreiminütigen Trickfilms an das Thema herangeführt. Matti vertraut darin seiner Freundin Flo an, dass er noch nicht Velo fahren kann. Als ihr das Geheimnis aus Versehen herausrutscht, wird Matti gehänselt, ehe die Geschichte ein versöhnliches Ende nimmt. Primarschülerinnen und Primarschüler lernen über Wimmelbilder mit Pausenhofszenen verschiedene Arten von Geheimnissen kennen. Da flüstert ein Junge einem Mädchen auf der Treppe etwas ins Ohr – vielleicht berichtet er ihr von seinem Schwarm – ein anderer sitzt mit hängendem Kopf alleine auf einer Parkbank. Was ihn bedrücken könnte, kann von den Unterrichtenden flexibel variiert werden; die Themenfelder reichen von Mobbing bis zu häuslicher Gewalt. Ein Mädchen weint und wird getröstet; vielleicht berichtet es zum ersten Mal von der Trennung seiner Eltern.

Die Kinder sollen lernen, dass die meisten Geheimnisse zu wahren sind und zur Privatsphäre gehören. Sie sollen aber auch erkennen, dass es solche gibt, welche man Lehrern oder Eltern anvertrauen darf, weil sie belastend oder gefährlich sind. In weiteren Lektionen diskutieren die Kinder etwa darüber, in welcher Situation eigene und fremde Daten wie die Lieblingsfarbe, die Namen der Geschwister oder das Familienfoto verwendet werden dürfen oder sie stellen sich mit Collagen selbst dar, um hernach einzuschätzen, was sie damit über sich preisgeben. Denn, was laut dem Lehrmittel selbst Erwachsene oft nicht wissen: Viele vermeintlich harmlose Bilder enthalten Informationen, weil sie etwa zeigen, wo die Person wann gewesen ist.

Der kantonale Datenschutzbeauftragte Bruno Baeriswyl machte bei der Präsentation vor den Medien deutlich, dass es beim Schutz der Privatsphäre um mehr geht, als kompetent mit Medien umzugehen oder bestimmte Einstellungen auf Facebook und Whatsapp anzuklicken: „Nur wer selbstbestimmt darüber entscheiden kann, was privat und was öffentlich ist, kann sein Leben eigenständig gestalten.“ Der Druck auf die Privatsphäre nehme zu und gerade junge Menschen müssten rechtzeitig verstehen, dass ihre persönliche Freiheit auf dem Spiel stehe. Beim Datenschutz gehe es, anders als es der Begriff vermuten lasse, nicht um den Schutz von Daten, sondern um den Schutz der Grundrechte von Personen, über die Daten vertrieben werden: „Ohne Datenschutz sind sie der Überwachung und der Manipulation ausgeliefert.“ Der Wert der Privatsphäre sei damit nicht nur ein individuelles Anliegen, sondern ein Fundament unserer liberalen Gesellschaft. Diesen Wert gelte es zuallererst zu vermitteln, ehe man auf den Schutz von Passwörtern oder Ähnliches verweise.

Der Rektor der Pädagogischen Hochschule Zürich, Heinz Rhyn, betonte, dass Fragen und Anliegen zur Privatsphäre und zum Datenschutz nicht nur die digitale Welt, sondern ganz verschiedene Lebensbereiche der Kinder durchdringen. Im neuen Lehrmittel würden diese aus rechtlicher, ethischer, pädagogischer und didaktischer Sicht beleuchtet. Dies sei der Mehrwert der erstmaligen Zusammenarbeit mit dem Datenschützer, die zwei Expertisen zusammenführt. Das Lehrmittel erfülle damit das Ziel des Lehrplans 21, der den Schulkindern das nötige Rüstzeug mitgeben wolle, um sich kritisch in die demokratische Gesellschaft einzubringen und eigenverantwortlich zu handeln.

Bereits 2011 hatte sich der eidgenössische Datenschutzbeauftragte im Rahmen der Kampagne „Meine Daten gehören mir!“ engagiert, wo sich 5- bis 14-Jährige über Online-Comics oder -Games dem Thema annähern können. Neu bei dem Angebot aus Zürich ist die Aufbereitung für den Unterricht und die altersgerechte Abstufung für eine Zielgruppe ab 4 Jahren. Man habe sich zwar an den Richtlinien eines EU-Handbuchs für den Unterricht zu Privatsphäre und Datenschutz orientiert, beim Erarbeiten der Materialien aber bei null beginnen müssen, weshalb die Projektpartner ihr Angebot als Pionierleistung ansehen. Andere Kantone hätten bereits Interesse an einer Übernahme signalisiert.

Das E-Book mit den Unterrichtsmaterialien steht kostenlos zum Download bereit. Ab Frühling 2019 wird es in Zürcher Schulklassen erprobt und allenfalls nochmals verbessert, ehe es im Herbst in die Ausbildung von Lehrpersonen an der Pädagogischen Hochschule einfließt. In den folgenden zwei Jahren sollen unter dem Projekttitel „Selbstbestimmt digital unterwegs“ Lerninhalte für die nächsthöheren Altersklassen bzw. sogenannte Zyklen des Lehrplans 21 folgen. Ob die Lehrkräfte die Materialien im Unterricht anwenden, ist ihnen überlassen; deren Einsatz ist nicht obligatorisch (Schenkel, Weltneuheit aus Zürich: Wie Fünfjährige lernen sollen, ihre Privatsphäre und ihre Daten zu schützen, www.nzz.ch 28.01.2019).

Frankreich u. a.

Bayer-Tochter Monsanto führte politische Listen

Die Bayer-Tochter Monsanto hat 2016 geheime Listen über UnterstützerInnen und KritikerInnen in Frankreich geführt. Wie Medien berichteten, haben PR-Agenturen im Auftrag des Konzerns Informationen über zuletzt rund 200 Personen aus Wissenschaft, Politik und Journalismus gesammelt, insbesondere zu deren Haltung zum Unkrautvernichter Glyphosat und zur Gentechnik. Nach Bekanntwerden des Vorgangs entschuldigte sich Bayer umgehend für die Praxis. Dies sei nicht die Art, wie Bayer den Dialog mit unterschiedlichen Interessengruppen und der Gesellschaft suche: „Auch wenn es derzeit keine Hinweise gibt, dass die Erstellung dieser Listen gegen gesetzliche Vorschriften verstoßen hat, wird Bayer eine externe Anwaltskanzlei damit beauftragen, das von Monsanto verantwortete Projekt zu untersuchen und die erhobenen Vorwürfe zu bewerten.“ Die Kanzlei werde allen in den Listen aufgeführten Personen Auskunft darüber geben, welche Informationen über sie gespeichert wurden. 2016 war in der EU heftig über die neuerliche Zulassung des Monsanto-Wirkstoffs Glyphosat gestritten worden. Weil keine Einigung erzielt wurde, verlängerte die EU-Kommission die Zulassung um anderthalb Jahre bis Ende 2017. Im Mai 2016 war öffentlich geworden, dass der deutsche Dax-Konzern Bayer Monsanto kaufen will. Im Juni 2018 wurde Mon-

santo von Bayer für rund 63 Mrd. US-Dollar gekauft.

- Gegner- und Freundeslisten

Ein den berichtenden Medien zugespieltes Dokument, datiert auf Ende 2016, zeigt ein Koordinatensystem mit wichtigen Personen und Gruppen in der Glyphosat-Debatte, dazu die Logos von Monsanto und der PR-Agentur Publicis. Auf der waagrechten Achse ist die Haltung zu Glyphosat verzeichnet, auf der senkrechten der Einfluss. Einzelne Namen sind nicht zu sehen. Publicis-Chef Clément Léonarduzzi erklärte dazu, die „alte Mannschaft“ sei mit dem Vorgang befasst gewesen. Er habe davon erst nach seinem Amtsantritt erfahren. Publicis sei im Auftrag der PR-Agentur Fleishman Hillard tätig geworden. Fast alle Personen, die damit befasst waren, seien mittlerweile ausgeschieden.

Ein anderes Dokument stammt von Fleishman Hillard und listet rund 200 Personen auf. Je nach Haltung und Einfluss werden sie mit Noten von Null bis Fünf bewertet. Die Personen wurden auch in Gruppen eingeteilt: Verbündete, potenzielle Verbündete, die es zu rekrutieren gelte, Akteure, die zu „erziehen“ und solche, die „zu überwachen“ seien. Fleishman Hillard erklärte in Reaktion auf die Veröffentlichung, man habe keinerlei Kenntnis von rechtswidrigen Handlungen. Hanning Kempe, Chef der deutschen Fleishman-Tochter, wollte sich zu den Vorgängen in Frankreich nicht äußern. Auch diese arbeitete 2016 für Monsanto. Im Rahmen der Kommunikationskampagnen seien, wie üblich, Excel-Dateien mit den öffentlich zugänglichen Daten der Stakeholder erstellt worden, „aber keine privaten Geschichten“. Fleishman Hillard sitzt wie Monsanto in St. Louis in den USA, arbeitete lange für den US-Konzern und nun für Bayer. Bayer kündigte an, die Zusammenarbeit mit den betreffenden Dienstleistern vorerst auf Eis zu legen. Der für dieses Projekt zuständige Manager habe bereits kurz nach Abschluss der Übernahme von Monsanto das Unternehmen verlassen.

- Ermittlungen

Zu den „Opfern“ in Frankreich zählt die heute 65 Jahre alte Sozialistin und damalige französische Umweltministerin Ségolène Royal. Sie ist heute als „Botschafterin für die Arktis und die Antarktis“ aktiv. Sie wurde als „null beeinflussbar“ geführt. Royal kommentierte, der Fall sage viel aus über das Lobby-System: „Sie spionieren, infiltrieren, beeinflussen.“ Dieses absolut „schädliche System“ müsse bekämpft werden. Im Widerstand gegen Monsanto habe sie sich 2016 „ein wenig alleine gefühlt“. Sie forderte Behörden und Justiz auf, dem Vorgang nachzugehen. Auch andere Lobbyisten müssten überprüft werden; sie könne sich nicht vorstellen, dass Monsanto das einzige Unternehmen sei, das solche Methoden anwende.

Die Staatsanwaltschaft in Paris leitete ein Ermittlungsverfahren gegen Monsanto wegen illegaler Erfassung privater Daten ein. Sie reagierte damit auf eine Klage der Zeitung „Le Monde“ und eines Journalisten, dessen Name auf der Liste stand. Rund die Hälfte der auf der Liste geführten Personen sind den Berichten zufolge JournalistInnen. Die Vereine Foodwatch und Générations Futures, die gegen Pestizide in Lebensmitteln kämpfen, bereiten nach eigenen Angaben ebenfalls Klagen vor. Wie Foodwatch France auf seiner Internetseite berichtet, stehen Geschäftsführerin Karine Jacquemart und Kommunikationschefin Ingrid Kragl auf der Liste. Die Dokumente seien ein neuer Beleg dafür, dass „die Lobbyisten multinationaler Konzerne vor nichts zurückschrecken, um ihr Geschäft zu schützen“. Sie glaubten, dass sie sich nicht an die Vorschriften halten müssten: „Das ist skandalös.“ Mit der Übernahme von Monsanto für rund 63 Mrd. Dollar hat sich Bayer jede Menge Ärger eingekauft. In den USA waren bis Mitte April 2019 mehr als 13.400 Klagen wegen Glyphosat eingereicht. Wegen der Risiken der Übernahme und des Kursverfalls der Aktie hatten die Bayer-Aktionäre den Vorstand bei der Hauptversammlung Ende April 2019 nicht entlastet.

- Grüner PR-Mann

Bayer-Lobbyist Matthias Berninger bemüht sich nun um Glaubwürdigkeit und versprach „maximale Transparenz“ und ein „klares Wertekonzept“ – so wie es sich für den Leiter des neu geschaffenen Bereichs Public Affairs und Nachhaltigkeit bei Bayer gehöre. Es gebe eine Reihe von Beispielen, so Berninger im Fußballsprech, „in denen Monsanto nicht den Ball gespielt hat, sondern auf den Mann oder die Frau gegangen ist. Der Zweck heiligt nicht die Mittel.“ Berninger meinte, es sei „sehr wahrscheinlich“, dass auch in anderen europäischen Ländern solche Listen angelegt worden sind. Welche das sind, will Bayer jetzt untersuchen lassen. Höchstwahrscheinlich dürfte auch Deutschland dazugehören, denn auch für den deutschen Markt war Fleishman Hillard zuständig. Deutschland spielte eine wichtige Rolle bei der Frage, ob die EU die Zulassung für das von Monsanto vertriebene Unkrautvernichtungsmittel Glyphosat verlängert oder nicht. Seit Januar 2019 ist der Hesse Berninger bei Bayer und soll verloren gegangenes Vertrauen zurückgewinnen. Der heute 48-Jährige war mit 23 der bis dahin jüngste Abgeordnete und für die Grünen im Deutschen Bundestag, mit 29 Jahren wurde er der jüngste je berufene Parlamentarische Staatssekretär in Deutschland. Renate Künast hatte ihn 2001 ins Bundeslandwirtschaftsministerium geholt. 2007 wechselte der mehrfache Familienvater die Seite und wurde Lobbyist für den Schokoriegelhersteller Mars in den USA. Jetzt soll Berninger das Ruder bei Bayer herumreißen. Er erklärte nach Bekanntwerden der Monsanto-Listen bei seinem ersten öffentlichen Auftritt, dass Bayer solche Listen wie die von Monsanto nicht geführt hat und dass jetzt Schluss ist mit solchen Praktiken. Er habe einen „klaren Wertekodex“, betont Berninger, der noch heute Mitglied der Grünen ist. Seine Führung sei anders als das, „was wir in der Vergangenheit von Monsanto erlebt haben.“

Es sind nun insbesondere die Grünen, seit Jahren große Kritiker von Monsanto, die auf Transparenz bestehen. In einem Brief an Bayer-Chef Werner Bauer, der u. a. von Anton Hofreiter, Renate Künast und Friedrich Ostendorff unterzeichnet wurde, heißt es: „Wir fordern Sie auf, die Liste für Deutschland sowie alle anderen EU-Mitgliedstaaten offenzulegen und für die Betroffenen zugänglich zu machen. Darüber hinaus

erwarten wir Informationen darüber, was das Ziel dieser Auflistung war und welche Maßnahmen auf dieser Basis erfolgen sollten." Timo Lange von der Nichtregierungsorganisation Lobby-Control forderte Ähnliches: „Jetzt muss alles auf den Tisch. Listen über Journalisten und Politiker zu führen, die sich mit bestimmten Themen beschäftigten, gehöre zwar fast schon zum Alltagsgeschäft von Lobbyisten. Illegal sei das meistens nicht. Fraglich sei aber, ob und warum Monsanto private Informationen sammeln ließ: „Das ist zumindest moralisch zu hinterfragen." Frank Überall, Bundesvorsitzender des Deutschen Journalisten-Verbands (DJV) meinte: „Informationen über Journalisten zu sammeln und die Medienvertreter nach ihrer vermeintlichen Beeinflussbarkeit zu kategorisieren, ist absolut inakzeptabel." Das sei Medienmanipulation. „Auch mit Blick auf die laufenden Glyphosat-Prozesse muss man sich fragen, was für ein Wissenschaftsbild ein Konzern hat, der Forscher nach Gläubigen und Abtrünnigen unterteilt."

- ...und anderswo

Am 21.05.2019 teilte Bayer mit, dass die PR-Agentur Fleishman Hillard nicht nur in Frankreich, sondern auch in Deutschland, Italien, den Niederlanden, Polen, Spanien, in Großbritannien und im Umfeld der EU-Institutionen Listen erstellen ließ, die KritikerInnen aufführen. Der Chemiekonzern beauftragte die internationale Anwaltskanzlei Sidley Austin damit, die Betroffenen zeitnah zu kontaktieren und nach möglichen weiteren Listen zu suchen. Die Kanzlei mit Sitz in Chicago, die bereits für Bayer tätig war, beschäftigt nach eigenen Angaben 2.000 RechtsanwältInnen; die Untersuchung soll das Büro in Brüssel führen.

Monsanto ist kein Einzelfall. 2018 wurde bekannt, dass Volkswagen einen umstrittenen Zulieferer ausspähen ließ. Die Anwaltskanzlei Hogan Lovells International hatte den Recherche-Auftrag von VW erhalten und die Nachforschungen an einen „sehr professionellen Dienstleister" weitergegeben. Detektive sollten sich Informationen über die Firma Prevent aus Sarajewo beschaffen. Es wurde damit gerechtfertigt, dass in Krisenzeiten dies zu den Kernaufgaben anwaltlicher Tätigkeit gehöre und „üblich und legitim" sei.

Das soziale Netzwerk Facebook soll gemäß Medienberichten eigene Daten zur Ausspähung und Überwachung von JournalistInnen benutzen. PR-Berater Dirk Popp, der u. a. den Milchmillionär Theo Müller vertrat, meinte, es sei in der Wirtschaft üblich, sich mit seinen Kritikern zu beschäftigen. Andere „Cases", so sein Sprachgebrauch, waren Nokia in der Zeit, als das Bochumer Werk geschlossen wurde, oder die Fast-Food-Kette Burger King, die mit vielen Vorwürfen zu Hygiene und Arbeitsschutz zu kämpfen hatte. Selbstverständlich analysiere man, so Popp, Argumente von Politikern und Journalisten. Fragwürdig werde es, wenn Auflistungen Informationen enthalten, die nicht mehr mit dem Job oder dem spezifischen Projekt zu tun haben. Er arbeite nicht in dieser Grauzone: „Es gibt aber durchaus Lobby-Agenturen und Kanzleien, die sich in diesem Umfeld tummeln und beispielsweise Tiefenrecherchen erstellen oder sogar Detektive einsetzen". In Deutschland wäre das aber eher das Extrem. In den USA werde da schon mit härteren Bandagen gekämpft. Da gehöre es zumindest in Teilen zur Normalität, im Dreck zu buddeln und zu diskreditieren (Dostert, Auf der Liste, SZ 13.05.2019, 17; Jahberg, Skandal um Bayer-Tochter Hat Monsanto auch in Deutschland geheime Listen geführt?, www.tagesspiegel.de 13.05.2019; Balser/Fromm/Hägler, die im Dreck graben, SZ 18./19.05.2019, 28; Auch in Deutschland: Monsanto führte in sieben Ländern Listen mit Gegnern, www.faz.net 21.05.2019; Dostert, Viele Fragen, wenig Antworten, SZ 22.05.2019, 17).

Großbritannien

Millionenbußgeld gegen British Airways wegen Datenschutzpanne

Die britische Datenschutzbehörde (Information Commissioner's Office – ICO) hat gegen die Fluggesellschaft British Airways (BA) ein Bußgeld in Höhe von 183,39 Millionen Britische Pfund, umgerechnet etwa 204 Millionen Euro, wegen des Verstoßes gegen die Datenschutz-Grundverordnung (DSGVO) verhängt. Die Höhe der Strafe entspricht 1,5% des Umsatzes der BA im Geschäftsjahr 2018 weltweit. Die Airline will möglicherweise Widerspruch einlegen.

Bei einem Angriff hatten Cyberkriminelle 2018 persönliche Daten und Kreditkarteninformationen inklusive Sicherheitscodes (CVV-Nummern) von KundInnen abgezogen, die zwischen dem 21.08 und 05.09. ihre Flüge per Kreditkarte bezahlt hatten. Betroffen waren davon rund 500.000 Personen. Die Hacker hatten die Daten erbeutet, indem sie Anfragen an die Webseite der Fluglinie auf eine gefälschte Internetseite weiterleiteten. Nach Ansicht des ICO haben schwache Sicherheitsvorkehrungen bei der Airline den Datendiebstahl erst ermöglicht. Elizabeth Denham, Datenschutzbeauftragte und Chefin des ICO, erklärte: „Persönliche Daten von Menschen sind genau das – persönlich. Wenn eine Organisation sie nicht vor Verlust, Schaden oder Diebstahl schützen kann, ist das mehr als eine Unannehmlichkeit. Deshalb ist das Gesetz eindeutig – wenn Sie mit personenbezogenen Daten betraut sind, müssen Sie sich darum auch kümmern. Diejenigen, die das nicht tun, werden von meiner Behörde überprüft."

Alex Cruz, Chef der BA International Airlines Group (IAG), zeigte sich von der Entscheidung der ICO „überrascht und enttäuscht". Seinen Angaben zufolge seien die gestohlenen Daten nicht missbräuchlich verwendet worden. Willie Walsh, Chef des BA-Mutterkonzerns International Airlines Group (IAG), will das Bußgeld nicht hinnehmen und kündigte Maßnahmen dagegen an: „Wir werden alle geeigneten Schritte unternehmen, um die Position der Fluggesellschaft energisch zu verteidigen, einschließlich etwaiger erforderlicher Einsprüche. Die BA hatte den Datendiebstahl 2018 selbst öffentlich gemacht. Die Aktie der IAG gab am frühen Morgen der Bekanntgabe des Bußgeldes um etwa 1% nach (Bünte, Datenschutzpanne: British Airways soll etwa 204 Millionen Euro Strafe zahlen, www.heise.de 08.07.2019, Kurzlink: https://heise.de/-4465412; Teurer Datenklau, SZ 09.07.2019, 18).

Großbritannien

Pornoblock nicht datenschutzkonform und leicht umgehbar

In Großbritannien gilt vom 15.07.2019 an ein „Pornoblock“, der Nutzende von kommerziellen Online-Erotik-Angeboten dazu verpflichtet, altersüberprüfende Ausweiskontrollen durchzuführen. Bei Verstößen gegen die Vorschriften drohen Sanktionen. Der Pornoblock soll Kinder davon abhalten, Online-Inhalte für Erwachsene anzusehen. Als „legale“ Pornobetrachter müssen die Nutzer persönliche Aufzeichnungen einreichen, um ihr Alter zu beweisen. Es besteht die Gefahr, dass die dabei offenbarten personenbezogenen Daten in Verbindung mit den sexuellen Fantasien und Wünschen der Nutzenden missbraucht werden können.

Die Maßnahmen haben zu Kontroversen geführt, da befürchtet wird, dass das Altersüberprüfungssystem ein wichtiges Ziel für Hacker sein könnte, die nach Erpressungsmaterial suchen oder persönliche Daten stehlen möchten. Forschende warnen davor, dass die vorgeschlagenen Vorschriften zum Schutz dieser personenbezogenen Daten völlig unzureichend sind. Eine Studie des Digital Privacy Watchdog „Open Rights Group“ weist darauf hin, dass die anzuwendenden Datenschutzbestimmungen „vage, ungenau und größtenteils ein Kästchen“ sind. Ein Sprecher nannte den britischen Pornoblock eine „Zeitbombe für den Datenschutz“. Bei geschätzten 20 Millionen Erwachsenen in Großbritannien, die Pornos schauen – etwa zwei von fünf Erwachsenen – könnte dies gravierende Folgen haben. Jim Killock, Geschäftsführer der Open Rights Group erklärt: „Aufgrund des sensiblen Charakters von Daten zur Altersüberprüfung muss es einen höheren Schutzstandard geben als den, den die Datenschutzgesetze vorgeben. Der BBFC-Standard soll dies liefern.“ Das British Board of Film Classification (BBFC) ist verantwortlich für die Durchsetzung der neuen Bestimmungen, einschließlich der Sanktionierung von Websites, die keine Einschränkungen enthalten, und auch für die Durchsetzung etwaiger Datenschutzanforderungen. „Es handelt sich jedoch um einen freiwilligen Standard, der nur wenige Informationen über das angebotene Datenschutzniveau enthält und keine Möglichkeit bietet, Abhilfe zu schaffen, wenn Unternehmen sich nicht daran halten.“ Der Standard sei daher „sinnlos und irreführend“.

Die britische Regierung besteht jedoch darauf, dass die neuen Richtlinien erforderlich sind, um Kinder daran zu hindern auf Materialien für Erwachsene zuzugreifen. Ein Sprecher der Abteilung für Digital, Kultur, Medien und Sport erklärte Anfang 2019: „Dies ist ein weltweit führender Schritt, um unsere Kinder vor Inhalten für Erwachsene zu schützen, auf die derzeit viel zu einfach online zugegriffen werden kann.“ Gemäß einer YouGov-Umfrage waren sich rund 76% der britischen Öffentlichkeit der damals in Kürze in Kraft tretenden Altersüberprüfungen nicht bewusst. Die Kritik bemängelt, dass die Maßnahmen leicht umgangen werden könnten – sowohl durch Computer-versierte junge Menschen als auch durch solche, die aus Datenschutzgründen die Registrierung für die Online-Anzeige von Pornografie vermeiden möchten. So besteht z. B. die Möglichkeit der Verwendung eines virtuellen privaten Netzwerks (VPN), mit dem Benutzende in einem anderen Land und damit außerhalb der Reichweite der Registrierungsrichtlinie für Großbritannien angezeigt werden. Die Suche nach VPNs in der Google-Suchmaschine hat sich verdreifacht, nachdem die britische Regierung den Starttermin für die neuen Pornoblocking-Maßnahmen bekannt gegeben hatte (Der britische Pornoblock ist eine Zeitbombe für den Datenschutz, www.tekk.tv 21.06.2019).

Spanien

Bußgeld gegen Fußball-App-Betreiber

Wegen Datenschutzverstößen der „La Liga“-App hat die spanische Datenschutzbehörde AEPD gegen den Ausrichter der beiden spanischen Profifußballligen ein Bußgeld in Höhe von 250.000 Euro verhängt. Mit der App wird der Zugriff auf Positionsdaten und auf das Mikrofon des Handys nicht klar erläutert. Die Datenschutzbehörde sieht hierin einen Verstoß gegen das in der Datenschutz-Grundverordnung (DSGVO) geregelte Transparenzgebot. Der Ausrichter Liga Nacional de Fútbol Profesional (LFP), auch als „La Liga“ bekannt, will die gleichnamige App zwar anpassen, hat aber zugleich Widerspruch gegen das Bußgeld angekündigt.

Hintergrund des Verfahrens ist eine unsichtbare Funktion der App, mit der die Organisatoren der ersten beiden spanischen Ligen unlizenzierten Aufführungen der im Pay-TV übertragenen Spiele auf die Spur kommen wollten. Während der Spiele nahm die App, kombiniert mit den Ortungsdaten, ein Sample der Umgebungsgeräusche auf, um eventuell laufende Spielübertragungen zu entdecken. Wie bei Sky benötigen Betreiber von Gaststätten auch in Spanien besondere Lizenzen, um die Spiele öffentlich zeigen zu können. Mit der App soll der Pay-TV-Betrug bekämpft werden. Immer wieder prellen Sportkneipen und Übertragungsorte die Gebühr für die Lizenz, die zur öffentlichen Vorführung der Fußballturniere berechtigt. Nach Angaben der spanischen Liga entsteht dadurch ein jährlicher Schaden von 400 Millionen Euro.

Zwar müssen Nutzende die Nutzung zusammen mit der separat zu erteilenden Zustimmung zu den AGB explizit genehmigen und die Berechtigung für den Mikrofonzugriff lässt sich in den Android-Einstellungen auch widerrufen. Die App funktioniert laut „La Liga“ auch ohne diese Berechtigungen. Doch kritisierte die Datenschutzbehörde, dass der Verwendungszweck der erhobenen Daten nicht transparent genug gemacht worden sei. „La Liga“ hat nun angekündigt, die umstrittene Funktion aus der App zu entfernen. Dennoch will der Liga-Ausrichter gerichtlich gegen die Entscheidung der AEPD vorgehen und behauptet, die Datenschützer hätten die eingesetzte Technik nicht verstanden. Die Liga versicherte, immer „verantwortungsbewusst“ und „im Einklang mit dem Gesetz“ gehandelt zu haben. So aktiviere die App das Smartphone-Mikro nur zur Sendezeit der Ligaspiele. Es würden keine Gespräche oder zusammenhängende Audio-Da-

teien aufgezeichnet, sondern lediglich Fragmente. Über 99% der Daten würden verworfen. Nur 0,75% der erfassten Daten würden benötigt, um relativ sicher einschätzen zu können, dass im Umfeld eine Übertragung stattfindet. Diese Werte würden dann gehasht und abgeglichen. Das sei nicht umkehrbar und Rückschlüsse auf Stimmen oder Gespräche seien unmöglich. Dies habe auch ein externes Gutachten bestätigt. Wie lange „La Liga" bereits auf diese Art nach Pay-TV-Betrügern fahndet, ist unklar (Briegleb, App hört mit: Datenschützer verhängt DSGVO-Bußgeld gegen spanische Fußballliga, www.heise.de 12.06.2019, Kurzlink: https://heise.de/-4445151; Spanische Fußballliga belauschte Millionen Fans per App, www.t-online.de 12.06.2019).

Polen

Hohes Bußgeld wegen Verstoß gegen Informationspflichten

Der Präsident des Amtes für den Schutz personenbezogener Daten (UODO) hat gegen Bisnode Polska ein Bußgeld in Höhe von mehr als 943.000 Złoty, umgerechnet etwa 220.000 €, wegen Nichterfüllung der Informationspflichten gemäß Artikel 14 DSGVO verhängt. Bisnode Polska ist ein polnisches Tochterunternehmen des schwedischen Anbieters für digitale Wirtschaftsinformationen Bisnode AB, welcher im Geschäftsjahr 2017 einen Umsatz von 3,6 Mrd. Schwedischen Kronen, umgerechnet etwa 333 Mio. €, erzielte. Gemäß der Ansicht von UODO missachtete Bisnode Polska die DSGVO-Informationspflichten in Bezug auf fast 6 Millionen Menschen.

Das Unternehmen verarbeitet rund 6 Mio. Datensätze aus öffentlich zugänglichen Quellen, hierunter auch personenbezogene Daten hinsichtlich der Wirtschaftstätigkeit der betroffenen Personen. Die Pflicht aus Art. 14 DSGVO wurde nach den Feststellungen des UODO lediglich bei 680.000 Personen auf elektronischem Wege erfüllt, von denen eine E-Mail-Adresse in der Datenbank vorlag. Die restlichen gut 5,3 Mio. betroffenen Personen erhielten hingegen keine Information. Bisnode Polska berief sich bei der Nichterfüllung der Informationspflicht auf eine gesetzliche Ausnahme, wonach die Information nicht erteilt werden muss, wenn sich die Erteilung als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert (Art. 14 Abs. 5 lit. b DSGVO). Nach Ansicht des UODO war dies jedoch nicht gerechtfertigt; Bisnode Polska hätte der Informationspflicht auch in Bezug auf diese Personen nachkommen müssen (Hügel, Polnische Datenschutzbehörde: Erstes DSGVO-Bußgeld in Höhe von mehr als 200.000 €, www.anwalt.de 09.05.2019).

Griechenland

Staat versteigert Krankenakten

In Griechenland bietet der Staat zur Aufbesserung der öffentlichen Finanzen vertraulichste persönliche Daten, nämlich Krankenakten, zum Kauf an. Das Land befindet sich wegen der Überschuldung und wegen der durch die internationalen Kreditgeber ausgeübten Kontrolle in ständiger Geldnot und bietet zur Linderung in Auktionen Krankenakten an.

Mit einem Schreiben vom 05.04.2019 kündigte die „Unabhängige Behörde für Staatliche Einnahmen, Generaldirektion für Zoll und spezielle Verbrauchssteuern" unter der Protokollnummer DDDY 10509 13 EX 2019 mit der Ausschreibung 3942E eine Auktion zum Verkauf von medizinischen Krankenakten und Röntgenaufnahmen an. Zum Ersteigern angeboten wurden u. a. 23.000 Röntgenaufnahmen samt der Patientenakten, Bruttogewicht ungefähr 23.000 Kilogramm, Einstiegspreis 0,60 Euro pro Kilogramm, 2.000 Röntgenaufnahmen plus Patientenakten, Bruttogewicht ungefähr 2.000 Kilogramm mit einem Einstiegspreis von 0,80 Euro pro Kilogramm, 6.000 gemischte Patientenakten, die auch Röntgenaufnahmen enthalten, zum Kilopreis von 0,50 Euro oder 5.000 Akten mit Röntgenaufnahmen für 0,80 Euro das Kilogramm.

In der Ausschreibung ist ausdrücklich vermerkt, dass die jeweiligen Posten nur als Gesamtheit und ohne Aussortierung durch den Käufer abgenommen werden müssen. Im amtlichen Schreiben der eigens auf Druck der Kreditgebertroika installierten unabhängigen Behörde beruft sich diese auf eine nationale griechische Datenschutzverordnung aus dem Jahr 2005. Offenbar ist der „Unabhängigen Behörde für Staatliche Einnahmen", die frei von jeglicher Kontrolle durch die Regierung ist, die europaweit seit 2018 anzuwendende DSGVO unbekannt. Es ist nicht erkennbar, dass eine Kontrolle stattfindet, ob es sich bei den Auktionsteilnehmern tatsächlich um Recyclingunternehmer handelt, geschweige denn, ob der jeweilige Recyclingunternehmer den Datenschutz rechtskonform beachtet. Entscheidend für die Behörde ist nur die Zahlungsfähigkeit des Käufers, welche vom Käufer vor der Auktion mit einer Garantiehinterlegung nachgewiesen werden muss. Auch wie die sensiblen Akten transportiert, gelagert und von wem sie später zerstört werden, das ist den obersten griechischen Finanzeintreibern, die nur der Troika Rechenschaft ablegen müssen, offenbar egal.

Sollten die Höchstbietenden mit der inhaltlichen Verwertung der Akten eine zusätzliche Finanzquelle realisieren und würde dies bekannt, so droht für sie wahrscheinlich nur eine Steuernachzahlung, allerdings nur, wenn die auch insofern zuständige „Unabhängige Behörde für Staatliche Einnahmen" hellhörig wird (Aswestopoulos, Griechenland: Der Staat verkauft persönliche Krankenakten, www.heise.de 30.04.2019, Telepolis).

USA

Visum nur gegen Einblick in Social-Media-Konten

Seit Ende Mai 2019 gilt ein Erlass des US-amerikanischen State Departments, also des Außenministeriums, der für Menschen gilt, die sich um ein Visum bewerben, um längerfristig in den USA zu leben und zu arbeiten. Danach müssen diese alle Informationen offenlegen, die auf sozialen Medien von ihnen gesammelt wurden, egal, ob sie oder ihre Freunde damit einverstanden sind. Gerechtfertigt wird dies wie folgt: „Wir arbeiten permanent daran, Mechanismen zu finden, die unsere Prüfungsprozesse verbessern, um US-Bürger zu schützen

und zugleich die legale Einreise in die Vereinigten Staaten zu ermöglichen."

Die meisten europäischen BesucherInnen der USA sind hiervon nicht betroffen: Wer zum Beispiel als DeutscheR in den Vereinigten Staaten Urlaub machen will, braucht kein Visum. Es genügt, sich im Internet beim elektronischen Reisegenehmigungssystem (Esta) zu registrieren. Die Genehmigung gilt zwei Jahre, man darf sich insgesamt 90 Tage im Land aufhalten. Wer jedoch ein Visum beantragen möchte beziehungsweise zur Einreise beantragen muss, muss dem Ministerium künftig einen beträchtlichen Teil seiner sozialen Interaktionen zugänglich machen. Das State Department schätzt, dass jährlich ungefähr 14,7 Millionen Menschen betroffen sein werden. Insgesamt reisen pro Jahr rund 77 Mio. TouristInnen in die USA ein.

Schon bisher war es nicht ganz einfach, ein Visum zu beantragen. Man musste zum Beispiel seine sämtlichen Auslandsreisen und Adressen auflisten, was für ebenso reise- wie umzugslustige Menschen eine nervenaufreibende Aufgabe sein kann. Man brauchte Dokumente, Führungszeugnisse, Geburtsurkunden; schließlich führte man ein persönliches Interview mit einem Konsularbeamten, dem allein es oblag, dem Antrag stattzugeben oder nicht. Es mag nachvollziehbar sein, dass ein Gastland eine ungefähre Idee von der Person haben will, die sich dort längere Zeit aufhalten möchte. Die neuen Regeln gehen allerdings einen Schritt weiter. Wer seine Interaktionen auf sozialen Medien offenlegt, wer seine E-Mails freigibt und seine Telefonnummern, der gibt in aller Regel nicht nur über sich selbst Auskunft, sondern auch über Bekannte und Freunde, über die Familie, also über persönliche Verbindungen. Zudem können hieraus z. B. kulinarische und sonstige unerhebliche Vorlieben ebenso wie politische Ansichten erkannt werden.

Der Erlass provozierte bisher kaum Protest in den USA. Manche ExpertInnen warnen davor, dass die Maßnahme vor allem dazu führe, dass Menschen sich in den sozialen Medien nicht mehr als die zeigten, die sie sind, dass sie sich selbst zensierten, um bei einer möglichen Überprüfung nicht unangenehm aufzufallen. Dass eine staatliche Behörde gezielt die Konten überprüft, mithin bei vielen Menschen deren Verbindung zur Welt, hat eine neue Dimension. Bisher gab es in den USA diese Art der Überprüfung von Konten in sozialen Medien, von E-Mails und von Telefonen für Menschen, die in Teilen der Welt unterwegs waren, in denen Netzwerke oder Regime das Sagen haben, welche die amerikanischen Behörden als terroristisch einstufen. Nun gilt dies, mit wenigen Ausnahmen für Diplomaten und andere Offizielle, für alle (Zaschke, Mein Konto, meine Kontakte, meine Mails, SZ 05.06.2019, 8).

USA

FTC verhängt Milliardenstrafe an Facebook wegen Cambridge Analytica-Fall

Die Federal Trade Commission (FTC), die US-amerikanische Verbraucherschutzbehörde, hat das soziale Netzwerk Facebook wegen der Ermöglichung des Datenmissbrauchs durch die britische Firma Cambridge Analytica zu einer Rekordstrafe von rund 5 Milliarden Dollar verdonnert. Der Konzern einigte sich mit der FTC auf einen entsprechenden Vergleich, unter anderem, um die Untersuchung des Cambridge-Analytica-Skandals zu beenden. Die politische Beratungsfirma hatte über eine Fragebogen-App („Thisisyourdigitallife“) unrechtmäßig Zugriff auf die persönlichen Daten von mehr als 80 Millionen Facebook-Nutzenden gehabt.

Ein Assistenzprofessor für Psychologie an der Universität in Cambridge, Aleksandr Kogan, hatte die App für seine Firma Global Science Research entwickelt. Ihr einziger Zweck war, Daten von möglichst vielen Menschen zu sammeln. Über eine Schnittstelle für Drittanbieter war dies damals über Facebook sehr einfach möglich. Facebook gibt an, Kogan habe behauptet, die Daten für wissenschaftliche Zwecke zu sammeln. In Wirklichkeit gingen sie aber auch an Firmen wie Cambridge Analytica, die sie benutzten, um sehr spitze Zielgruppen zu bilden, die auf für sie zugeschnittener Werbung ausgesetzt wurden (Microtargeting). Die Zielgruppen wurden mithilfe von psychologischen Persönlichkeitsprofilen gebildet, die aus den Daten von Kogans App stammten. Die App wurde von 270.000 US-AmerikanerInnen genutzt. Besonders problematisch war, dass es Facebook erlaubte, auch die Daten von „Freunden“ der App-Nutzer abzuschöpfen. Auch wer die App gar nicht selbst nutzte, aber mit einem der Nutzer befreundet war, wurde somit zum Opfer des Skandals. So kam es zu der hohen Zahl von 87 Mio. Profilen. Es handelt sich also nicht um ein Datenleck, etwa durch eine Attacke auf Facebook. Vielmehr war es ganz offiziell vorgesehen, dass die Daten über eine Schnittstelle abfließen konnten. Und - das ist der Hauptvorwurf gegen Facebook - was dann damit geschah, habe Facebook viel zu lax kontrolliert. Zwar hatte das soziale Netzwerk untersagt, dass Daten weitergegeben werden dürften, überprüfte das allerdings nicht wirksam.

Zusätzlich zu der Strafe habe, so Medienberichte, Facebook zugestimmt, umfassender zu dokumentieren, wofür Nutzerdaten genutzt und an wen sie weitergegeben werden. Was genau diese neuen Regularien vorschreiben sollen, ist bisher unklar. Facebook gelang es offenbar, größere Einschränkungen zu vermeiden, was das Sammeln von Daten und das Teilen mit Drittanbietern angeht. Das US-Justizministerium muss dem Vergleich zustimmen. Gemäß den Berichten ging die 3:2-Entscheidung, dem Vergleich mit Facebook zuzustimmen, auf die Republikaner zurück, die in dem fünfköpfigen Gremium an der Spitze der FTC in der Mehrheit sind. Die beiden oppositionellen Demokraten wollten Facebook rigidere Datenschutzregeln auferlegen.

Die Strafe ist mit weitem Abstand die höchste Strafe, welche eine US-amerikanische Behörde jemals gegen einen Digitalkonzern verhängt hat. Verglichen mit Facebooks Umsatz und Gewinn, erscheint sie weniger groß: Facebook erzielte im Jahr 2018 einen Gewinn nach Steuern von mehr als 22 Milliarden Dollar bei einem Umsatz von fast 56 Milliarden. Im ersten Quartal 2019 meldete der Konzern einen Gewinn von 2,4 Milliarden Dollar, nachdem er für eine mögliche Strafe der FTC schon eine Rückstellung in Höhe von 3 Milliarden gebildet hatte. Der Konzern ver-

fügt über Barreserven von 40 Milliarden Dollar. Auch die Anleger hatten offenbar mit einem gravierenderen Ende der FTC-Untersuchung gerechnet; Facebooks Aktienkurs stieg nachbörslich nach Bekanntwerden der Strafe an.

Entsprechend kritisch kommentierten insbesondere demokratische PolitikerInnen die Entscheidung der Behörde. Der Kongressabgeordnete und Facebook-Kritiker David Cicilline schrieb auf Twitter: „Die FTC hat Facebook gerade fünf Monate zu früh ein Weihnachtsgeschenk gemacht“. Elizabeth Warren, prominente Präsidentschaftsbewerberin des linken Parteiflügels, setzte nach: „Der Konzern ist für eine Beaufsichtigung zu groß, und diese Körnchen-im-Sand-Strafe bestätigt das. Die FTC sollte Facebook schlicht und einfach zerschlagen. Genug ist genug“. Auch andere Präsidentschaftsbewerber der Demokraten vertreten im zurzeit laufenden Vorwahlkampf eine harte Linie gegenüber Facebook und haben schon mehrfach eine Zerschlagung des Konzerns ins Gespräch gebracht. Der demokratische Senator Richard Blumenthal aus Connecticut meinte, eine ernstzunehmende Regulierung von Facebook hätte auch strukturelle Reformen umfassen müssen. So aber werde der Welt signalisiert, dass der Datenschutz in den USA ein Papiertiger sei. Aber auch Präsident Donald Trump, in dessen eigenem Wahlkampf die Daten benutzt wurden, ist nicht besonders gut auf die IT-Konzerne zu sprechen, weil er sich von diesen unfair behandelt fühlt.

Allerdings ist die Sache für Facebook noch nicht ausgestanden. Der Generalstaatsanwalt des District of Columbia, Karl Racine, hat gegen Facebook im Dezember 2018 wegen des Cambridge-Analytica-Falls Klage erhoben. In Deutschland geht das Bundeskartellamt gegen Facebook vor. Milliardenstrafen gegen Tech-Konzerne kennt man bisher nur aus Europa, wo unter der Wettbewerbskommissarin Margarethe Vestager allein der Google-Konzern schon knapp 7 Mrd. Euro an Bußgeld zahlen musste. In den USA war die höchste Strafzahlung vor der Facebook-Einigung 22 Mio. Dollar gewesen, die sich auch gegen Google richtete (Benrath, „Genug ist genug!“, www.faz.net 14.07.2019; Martin-Jung, Angriff auf die Sammler, SZ 15.07.2019, 15).

USA

Wegen Verstoß gegen Kinder-Datenschutz Millionenstrafe für Musical.ly

Wegen Verstoß gegen den Datenschutz für Kinder muss die durch TikTok ersetzte Firma Musical.ly für das Angebot ihrer Karaoke-App 5,7 Millionen US-Dollar (ca. 5 Mio €) Strafe zahlen. Nach Angaben der für das Verfahren verantwortlichen Handelsbehörde FTC basiert die Geldstrafe gegen den Betreiber der Lip-Sync-App auf einem gerichtlichen Vergleich mit Musical.ly. Es handele sich bisher um die höchste Geldstrafe für Verletzung des Gesetzes COPPA (Children’s Online Privacy Protection Act). Außerdem muss Musical.ly Daten in großem Umfang löschen, darunter alle Videos, die von Kindern hochgeladen wurden.

Das US-Bundesgesetz COPPA erlaubt zwar kontext-orientierte Reklame, verbietet aber Werbung, die sich am Verhalten der Kinder (Personen unter 13 Jahren) orientiert. Daher wird das Sammeln personenbezogener Daten untersagt, wenn sich damit Kind, Gerät oder Konto wiedererkennen lassen. Unter anderem ist es rechtswidrig, folgende Daten zu erheben, wenn sich eine App (auch) an Kinder richtet, sofern die Erziehungsberechtigten nicht im Voraus verifizierbar zugestimmt haben: Namen oder Usernamen, Kontaktdaten, Gerätekennzeichnungen, Adressen oder Ortsdaten auf Straßenebene, Fotos, Videos oder Tonaufnahmen des Nutzers.

Der FTC-Vorsitzende Joe Simons erklärte: „Die Betreiber von Musical.ly – inzwischen als TikTok bekannt – wussten, dass viele Kinder die App nutzten, haben aber dennoch dabei versagt, vor dem Sammeln von Namen, E-Mail-Adressen und anderen persönlichen Daten von Nutzern unter 13 Jahren die Zustimmung der Eltern einzuholen. Die Rekordstrafe sollte eine Erinnerung an alle Online-Dienstleister und Webseiten sein, die sich an Kinder richten. Wir nehmen die Durchsetzung von COPPA sehr ernst, und wir werden Firmen nicht tolerieren, die das Gesetz schamlos ignorieren.“ Der Musical.ly-Betreiber habe gewusst, dass ein signifikanter Prozentsatz der UserInnen unter 13 Jahre alt war. Außerdem habe es tausende Beschwerden von Eltern gegeben; das Unternehmen habe die Daten länger gespeichert als notwendig.

Angegriffen wurde zudem, dass die Nutzungsprofile automatisch öffentlich waren, sodass jede andere UserIn Angaben über Kinder samt Fotos und Videos sehen konnte. Selbst nach Änderung der Voreinstellung blieben Bilder und Kontaktmöglichkeit öffentlich. Die FTC verweist in diesem Zusammenhang auf Berichte, wonach Erwachsene über Musical.ly Kontakt zu Kindern gesucht haben. 2017 hat das chinesische Medien-Unternehmen Bytedance Musical.ly übernommen. 2018 mussten dann die Musical.ly-Nutzenden zu TikTok umziehen, einer ähnlichen App von Bytedance mit damals über einer halben Milliarde monatlichen UserInnen. Musical.ly war 200 Millionen Mal installiert worden. US-UserInnen hatten bei Musical.ly nicht weniger als 65 Millionen Konten eingerichtet. Das Gerichtsverfahren „USA v. Musical.ly“ wird beim US-Bundesbezirksgericht für den Hauptstadtbezirk District of Columbia geführt (Az. 2:19-cv-1439). Das Urteil auf Grundlage des geschlossenen Vergleichs gilt als Formsache (Sokolov, Kein Datenschutz für Kinder: Millionenstrafe für Musical.ly, www.heise.de 28.02.2019, Kurzlink: https://heise.de/-4322211).

USA

Humanyze u. a. für mehr Mitarbeitertracking

Einige Start-ups arbeiten an Systemen, mit denen sich Beschäftigte minutiös überwachen lassen. Wer im Logistikbereich tätig ist, ist einer massiven Überwachung seiner Tätigkeit durch den Arbeitgeber ausgesetzt. Doch auch im Büro drohen einem Bericht auf „Technology Review“ zufolge solche Trackingmaßnahmen.

Das IT-Marktforschungsunternehmen Gartner hat im Rahmen einer Umfrage 2018 ermittelt, dass 22% der weltweit agierenden Wirtschaftsunternehmen in unterschiedlichen Industrien aufzeichnen, wo sich ihre Angestellten gerade befinden. 17% überwachen die Computernutzung und 16% kontrollieren die E-Mails (Microsoft Outlook) oder die Kalender. Das Management der Unter-

nehmen gibt jeweils an, dass dies mit dem Ziel der Erhöhung der Produktivität erfolge. Start-ups arbeiten daran, dass Mitarbeitende noch genauer überwacht werden – in Form eines „Fitbits für Deine Karriere", so deren Werbeslogan. Die US-Firma Humanyze arbeitet seit 2014 an einem sogenannten Smart Badge, den die Beschäftigten um den Hals tragen sollen. Dieser soll über 40 verschiedene „Datenpunkte" („Datenabgase") erfassen können, die Angestellte hinterlassen und die sich als wertvoll erweisen können.

Das am MIT entstandene Unternehmen erfasst z. B., wenn ein Angestellter redet, sich bewegt oder am Schreibtisch sitzt. Der Smart Badge erkennt, wenn sich andere Nutzende mit Badge in der Nähe befinden; er trackt sogar Toilettengänge. Die Firma betont, Unternehmen erhielten nur aggregierte Daten, sie können also beispielsweise nicht einzelnen Gesprächen der Mitarbeiter folgen. Es würden Daten generiert, die zur Optimierung von Firmenabläufen führen sollen. So habe sich, gemäß Firmenchef Ben Waber, ein ehemaliger Doktorand am MIT Media Lab, durch die Datenerfassung etwa gezeigt, dass größere Kantinentische die Leistung einer Programmierertruppe um bis zu 10% steigern könnten. Wer statt an Vierer- an Zwölfertischen sitzt, codet angeblich besser, weil es mehr Interaktionen gibt (*Schwan,* Trend zum detaillierten Mitarbeitertracking, www.heise.de 13.05.2019, mehr dazu bei Technology Review Online Ein „Fitbit für Deine Karriere", Kurzlink: https://heise.de/-4404093):

Botswana

Gericht: Sex ist Privatsache

Ein Gericht in Botswana hat das Verbot gleichgeschlechtlicher sexueller Handlungen als verfassungswidrig eingestuft. Das Strafgesetzbuch in dem afrikanischen Land sah dafür bislang bis zu sieben Jahre Haft vor. Das Gesetz stammte aus der Zeit der britischen Kolonialherrschaft und wurde kaum angewendet. Das Gericht argumentierte, dass freiwillige sexuelle Handlungen zwischen Erwachsenen Privatsache seien und kein Thema für den Gesetzgeber. Homosexuelle Handlungen sind immer noch in zahlreichen Ländern Afrikas illegal. Für die Menschenrechtsorganisation Amnesty International ist das Urteil ein starkes Signal, dass niemand aufgrund seiner sexuellen Orientierung belästigt, diskriminiert oder kriminalisiert werden dürfe. Die Organisation für Lesben, Schwule und Bisexuelle in Botswana begrüßte das Urteil (Sex ist Privatsache, SZ 12.06.2019, 7).

Hongkong

Tests mit „intelligentem Gefängnis"

Hongkong will für seine rund 8.300 Inhaftierten in den Justizvollzugsanstalten das „Smart Prison" – das intelligente Gefängnis – einführen. Das Konzept des Correctional Services Department (CSD), zu dem Tests begonnen haben, zielt auf mehr Effizienz und Sicherheit durch Technik und Innovation. Um zu verhindern, dass Inhaftierte sich mit Drogen vergiften und dadurch Schaden zufügen, soll z. B. ein Roboter den Kot der Gefangenen auf Rauschmittel hin überprüfen. Gefangene würgen vor Haftantritt Drogen gut verpackt herunter und ziehen sie im Gefängnis wieder aus ihren Exkrementen. 2018 wurden 25-mal Drogen beschlagnahmt; in 16 Fällen hatten die Häftlinge diese in „Körperhöhlen" versteckt. Im gleichen Jahr kam es in 48 Fällen zu Selbstverletzungen, so der CSD: „Leider sind zwei Personen im Gewahrsam trotz der unermüdlichen Bemühungen der Mitarbeiter gestorben." Das Smart Prison setzt nun auf Bewegungsmelder und Armbänder. Mit Letzteren soll das Wachpersonal den Puls der Insassen beobachten können. Ist er nicht normal, wird Alarm ausgelöst. Zum Konzept gehören auch „intelligente Kameras", die in einer Haftanstalt mit der niedrigsten Sicherheitsstufe in der Kleinstadt Pik Uk im Osten von Hongkong ausprobiert werden. Pro Zelle sind zehn Kameras installiert, zwei weitere auf der Toilette. Die „intelligente" Technik weiß, wie sich ein Insasse normalerweise bewegt und gibt Alarm, wenn einer beispielsweise seinen Kopf gegen die Wand schlägt. Gemäß einer Zeitungsbericht äußerte sich ein Abgeordneter im Parlament dazu: „Ob die Daten gespeichert und missbraucht werden können, ist ein heikles Thema" (Holzki, Smart Home, smart Knast, SZ 22.05.2019, 1).

Technik-Nachrichten

Youtube koppelt per Algorithmus Erotik mit Kinder-Videos

In den vergangenen 18 Monaten zeigte sich verstärkt, dass Zuschauende bei Youtube über die Funktion „Nächstes Video" zu Desinformationskampagnen geleitet werden. So bekommen z. B. Kinder verstörende Videos angezeigt. Zwar hatte die Plattform Januar 2019 angekündigt, seine Empfehlungsmechanismen zu ändern. Doch zeigen Berichte von Forschenden am „Berkman Klein Center for Internet and Society" der Universität Harvard auf, dass der Youtube-Empfehlungsalgorithmus z. B. ZuschauerInnen von erotischem Content auf Videos weiterleitet, die leicht bekleidete Teenager oder auch Kinder in Badesachen oder beim Spagat zeigen. Reporter Max Fisher kommentierte: „Jedes Video mag für sich genommen unschuldig erscheinen. Ein Heimvideo eines Kindes in einem zweiteiligen Badeanzug oder Schlafanzug. Aber jedes hat drei gemeinsame Eigenschaften: Das Mädchen ist weitgehend unbekleidet oder kurz nackt zu sehen. Sie ist nicht älter als acht Jahre. Ihr Video wird stark vom Youtube-Algorithmus angepriesen."

Eine brasilianische Mutter fand so heraus, warum ein eigentlich langweiliges Video ihrer Tochter inzwischen mehr als 400.000 Aufrufe hat. Nachdem Youtube mit den problematischen Video-Ketten konfrontiert worden war, stellte der Al-

gorithmus andere Empfehlungen zusammen. Das Thema firmiert unter dem Schlagwort „Softcore-Pädophilie". Im Februar 2019 hatte der Youtuber Matt Watson herausgefunden, dass pädophile Nutzer die Kommentarspalten von Videos nutzen, um zum Beispiel auf Szenen kleiner Mädchen hinzuweisen, die diese beim Spagat zeigten. Der Algorithmus der Seite hatte bei entsprechendem Nutzungsverhalten solche Inhalte schnell auch als „Nächstes Video" vorgeschlagen.

Daraufhin hatten gemäß Medienberichten Firmen wie Disney, Nestle und der Fortnite-Produzent Epic Games Werbekampagnen vorläufig gestoppt. Youtube schaltete daraufhin die Kommentare bei Millionen von Videos mit kleinen Kindern ab und löschte 400 Kanäle. Außerdem reduzierte Youtube die Werbemöglichkeiten und die Auffindbarkeit von Videos Minderjähriger in „riskanten Situationen". Nach Veröffentlichungen hierzu im Mai 2019 betonte die Youtube-Sicherheitsbeauftragte Jennifer O'Connor in einem Blogeintrag, dass der Kinderschutz „die höchste Priorität" genieße. Neben den bereits bekannten Maßnahmen habe die Google-Tochter allein im ersten Quartal 2019 in diesem Zusammenhang 800.000 Videos gelöscht, die meisten, bevor sie mehr als ein Dutzend Mal angesehen wurden. Zudem habe man in den vergangenen Monaten festgelegt, Livestreams von Minderjährigen nur noch in Begleitung von Erwachsenen zu erlauben.

Die Erwachsenenklausel trägt der Tatsache Rechnung, dass „Familien-Vlogging" sich als erfolgreiches Genre etabliert hat. Eltern stellen dabei in der Regel inszenierte Videos aus dem Familienleben online und schaffen es in einigen Fällen, gemeinsam mit ihrem Nachwuchs zu Influencern zu werden und Partnerverträge mit Youtube abzuschließen. Diese Content-Produzenten sehen Kommentare und Empfehlungen in der Kategorie „Nächstes Video" als Möglichkeit zur Reichweiten- und damit zur Werbeeinnahmesteigerung. Dem entsprechend kritisch werden von dieser Gruppe mögliche Einschränkungen der Funktionen beäugt. Gemäß Youtube folge man wegen dieser „Produzenten" nicht dem Wunsch, das Empfehlungssystem für Kindervideos komplett auszuschalten. Die Technologie zur Identifizierung würde allerdings existieren. Ein anderer Faktor ist das fehlende Bewusstsein bei Nutzern: Eltern, die Videos ihrer Kinder für Verwandte oder Bekannte oder ohne feste Zielgruppe hochladen, markieren das jeweilige Video nicht als privat, was zur Folge hätte, dass es nur per Direktlink aufrufbar wäre.

Youtube richtete seinen Algorithmus lange völlig hemmungslos auf drei Ziele aus: höchstmögliche Video-Aufrufzahlen, maximale Verweildauer und möglichst viele Interaktionen wie Likes und Kommentare. Mehrere Ex-Mitarbeiter von Youtube berichteten, dass der Strudel, der Nutzende geräuschlos in dunkle Gefilde führt, intern früh und mehrmals angesprochen worden sei. Youtube-Chefin Susan Wojcicki und das Management hätten das Thema aber abmoderiert, um das Wachstum nicht zu gefährden. Die Firma bestreitet diese Darstellung. Google verhält sich, so Chris Stokel-Walker, der ein Buch über die Plattform geschrieben hat, reaktiv: „Sie nehmen jeden Skandal, wie er kommt, und versuchen die Sachen zu reparieren, wenn sie passieren" (Kuhn, „Nächstes Video", SZ 05.06.2019, 19).

Rechtsprechung

BVerwG

Für private Videoüberwachung gilt nur die DSGVO

Das Bundesverwaltungsgericht (BVerwG) hat mit Urteil vom 27.03.2019 klargestellt, dass die Videoüberwachung durch private Stellen ausschließlich am europäischen Datenschutzrecht zu messen ist (Az.: 6 C 2.18): „Eine Privatperson kann sich nicht selbst zum Sachwalter des öffentlichen Interesses erklären. Insbesondere ist sie nicht neben oder gar anstelle der Ordnungsbehörden zum Schutz der öffentlichen Sicherheit berufen." Neben der Datenschutz-Grundverordnung (DSGVO) gebe es insofern keinen „Raum für eine künftige Anwendung" des 2017 vom Bundestag beschlossenen sogenannten Videoüberwachungsverbesserungsgesetzes. Die Videoüberwachung durch Private ist demgemäß in der DSGVO abschließend geregelt. Danach müsse die mit einer Überwachungskamera ermöglichte Datenverarbeitung „erforderlich für die Wahrnehmung einer Aufgabe sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde". Eine zusätzliche Abwägung mit den Interessen der Betroffenen ist nicht vorgesehen.

In dem zugrunde liegenden Fall geht es um eine Anordnung der brandenburgischen Datenschutzbeauftragten Dagmar Hartge zur rechtskonformen Videoüberwachung in einer Zahnarztpraxis. Die Klägerin, eine Zahnärztin, hatte oberhalb des unbesetzten Empfangstresens eine Digitalkamera installiert, die laufende Bilder in Echtzeit herstellt. Die Bilder konnten auf Monitoren angesehen werden, die die Ärztin in den Behandlungszimmern aufgestellt hatte. Sie hatte geltend gemacht, der ungehinderte Zugang zu ihrer Praxis könne ausgenutzt werden, um dort unerkannt Straftaten zu begehen.

Das Oberverwaltungsgericht Berlin-Brandenburg (OVG) hatte im Berufungsverfahren mit Urteil vom 06.04.2017 aber keine Tatsachen festgestellt, wonach eine erhöhte, über das allgemeine Lebensrisiko hinausgehende Gefährdungslage bestehen könnte (OVG 12 B 7.16). Ihm zufolge gab es keine tatsächlichen Anhaltspunkte, die darauf hindeuten, die Praxis könne während der Öffnungszeiten Tatort für Einbrüche, Überfälle und Gewalttaten werden. Das Gebäude liege nicht in einem Gebiet mit erhöhtem Gefahrenpotenzial. Personen könnten auch durch das Betreten des überwachten Raums nicht rechtswirksam ihr Einverständnis mit der Maßnahme zum Ausdruck bringen.

Hartge hatte die Klägerin verpflichtet, die Kamera so auszurichten, dass sie den öffentlich zugänglichen Bereich der Praxis nicht erfasst. Das BVerwG bestätigte, dass dieses Vorgehen „verhältnismäßig, insbesondere geeignet und erforderlich" war. Es habe sich um das „mildere Mittel gegenüber einem Abdecken oder Abbau der Kamera" gehandelt. Zudem sei die Anordnung auch von der seit 25.05.2018 unmittelbar in allen EU-Mitgliedstaaten geltenden DSGVO gedeckt. Danach kann die Aufsichtsbehörde einen Verantwortlichen anweisen, Verarbeitungsvorgänge auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der Verordnung zu bringen.

Videoaufnahmen sind gemäß dem Urteil allein an Art. 6 DSGVO zu messen, nicht jedoch an der nationalen Umsetzung in § 4 BDSG, der mit dem Videoüberwachungsverbesserungsgesetz verschärft wurde, was u. a. von der DVD und dem Netzwerk Datenschutzexpertise kritisiert wurde (vgl. DANA 4/2016, 188 ff.). Die Verschärfung war vor allem eine Reaktion auf einen Amoklauf 2016 in einem Münchner Einkaufszentrum mit neun Toten. Mit der damit verknüpften Reform des Bundesdatenschutzgesetzes sollten mehr Kameras an „öffentlich zugänglichen großflächigen Anlagen" angebracht werden dürfen. Das Parlament wollte damit die Sicherheit vor allem in Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen sowie in Einrichtungen und Fahrzeugen des öffentlichen Personennahverkehrs erhöhen.

Gemäß dem BVerwG ist bedeutsam, ob die Datenverarbeitung „für die Verhinderung von Straftaten unbedingt erforderlich ist", ob sie absehbar, also branchenüblich sei, oder ob die Betroffenen in der konkreten Situation „vernünftigerweise damit rechnen müssen, dass ihre Daten verarbeitet werden". Die Videoüberwachung des öffentlich zugänglichen Bereichs der Praxis sei so unzulässig, „weil sie nicht erforderlich ist, um berechtigte Interessen der Klägerin zu wahren".

Die Entscheidung des BVerwG bestätigt die Auffassung der Datenschutzaufsichtsbehörden. Der Hamburgische Datenschutzbeauftragte Johannes Caspar begrüßte deshalb auch die klare Ansage des Gerichts, da „die Aufgabe der Videoüberwachung zum Schutz der öffentlichen Sicherheit nicht auf private Betreiber übertragen werden" könne. Letztere könnten zwar auch nach Maßgabe der DSGVO „die Schutzinteressen von dritten Personen bei der Datenverarbeitung berücksichtigen". Dabei gebe es aber keine „nationalen Vorrang- und Verstärkerklausel zum Schutz der öffentlichen Sicherheit durch private Videoüberwachungsanlagen". Gegen das nun zumindest für den Privatbereich für nicht anwendbar erklärte Gesetz ist auch noch eine Verfassungsbeschwerde von Mitgliedern der Piratenpartei anhängig (Krempl, Bundesverwaltungsgericht: Gesetz für mehr Videoüberwachung ist nicht anwendbar, www.heise.de 31.05.2019, Kurzlink: https://heise.de/-4436026).

Bayerischer VGH

Grunddaten für Mietspiegel müssen offengelegt werden

Gemäß einem Urteil des Bayerischen Verwaltungsgerichtshofes in München (VGH) vom 13.05.2019 muss die Stadt München dem Haus- und Grundbesitzerverein München (kurz: Haus und Grund) Daten zugänglich machen, die dem kommunalen Mietspiegel zugrunde liegen (Az. 4 B 18.1515). Haus und Grund wurden in dem Verfahren Ansprüche zugesprochen, die Nettokaltmiete pro Quadratmeter und den Stadtteil der 3322 Wohnungen zu erfahren, die in den Mietspiegel 2017 eingeflossen sind. Den Antrag, die genaue Lage der Wohnungen zu erfahren, wies das Gericht zurück. Außerdem bekommt der Verband Zugang zu Angaben über 30.000 Wohnungen, die als nicht mietspiegelrelevant gelten. In erster Instanz hatte das Verwaltungsgericht (VG) der Stadt Recht gegeben, die die Herausgabe mit Verweis auf den Datenschutz abgelehnt hatte. In der mündlichen Verhandlung betonten die Richter des VGH, „dass das für amtliche Befragungen geltende Statistikgeheimnis strikt einzuhalten sei", weshalb der Klage von Haus und Grund nur teilweise stattgegeben wurde. Aber es könne nicht sein, „dass der Mietspiegel komplett nicht-überprüfbar ist".

Die Leiterin des Sozialreferats der Stadt München, Dorothee Schiwy, will auf Basis der Urteilsbegründung das weitere Vorgehen prüfen. Sie forderte Haus und Grund auf, „die seit Jahren andauernde Agitation gegen den Mietspiegel einzustellen". Man müsse „sich schon fragen, welche Ziele jemand wirklich verfolgt, der behauptet, der Mietspiegel sei zu niedrig – und das in einer Zeit, in der Menschen reihenweise die Stadt verlassen, weil sie sich die Mieten nicht mehr leisten können". Das sei „schlicht unmoralisch". Vorwürfe, der Mietspiegel sei manipuliert, seien „haltlos". Auch Linke und SPD kritisierten Haus und Grund wegen seines „Feldzugs gegen den Mietspiegel".

Die Erstellung des Mietspiegels basiert auf Bundesrecht. Demnach dürfen nur Wohnungen eingehen, die in den vergangenen vier Jahren neu vermietet worden sind oder deren Miete verändert worden ist. Wohnungen mit älteren Verträgen und geförderte Wohnungen sind ausgeschlossen. Dem Mietspiegel 2017 zufolge, den die Meinungsforscher von Kantar TNS und das Statistik-Institut der Ludwig-Maximilians-Universität im Auftrag der Stadt erstellt haben, lag die durchschnittliche Nettokaltmiete bei 11,23 € (im Mietspiegel 2019 sind es 11,69 €).

Rudolf Stürzer, der als Vorsitzender von Haus und Grund München ca. 30.000 Mitglieder vertritt, äußerte den Verdacht, dass die Stadt aus politischen Gründen für eine Auswahl sorge, die den Mietspiegel nach unten verzerre. Das Urteil ist für ihn eine Bestätigung, „dass wir Licht ins Dunkel des Mietspiegel bringen können". Wenn man die Daten bekomme, werde man sie „einem Sachverständigen geben, der sie auf Plausibilität und Repräsentativität prüft. Wenn herauskommt, dass alles seine Richtigkeit hat, ist das okay". Das Vorgehen von Haus und Grund stößt bei anderen Immobilienbesitzenden, dem 80.000 Mitglieder starken Eigenheimerverband Bayern, auf Kritik: Wer München „beim Mietspiegel durch Klagen einen Knüppel zwischen die Beine wirft, trägt dazu bei, dass in Zukunft die Mieten noch stärker steigen". Das sei nicht im Sinne der Menschen, die sich Wohneigentum zulegen wollen; mit den Mietpreisen stiegen nämlich auch die

Kaufpreise an (Krass, Urteil zu Daten für Mietspiegel, SZ 14.05.2019, 26).

VG Berlin

Schulsanktionen nach Videoveröffentlichungen auf Social Media

Im Rahmen von zwei Eilverfahren vom 07.06.2019 entschied das Verwaltungsgericht Berlin (VG), dass Schüler vorläufig vom Unterricht suspendiert werden dürfen, weil sie heimlich Videos und Fotos von Lehrkräften angefertigt haben, die dann auf Instagram veröffentlicht wurden (VG 3 L 357.19 / VG 3 L 363.19). Betroffen sind zwei Schüler einer zehnten Klasse einer Integrierten Gesamtschule in Berlin, die die heimlich erstellten Videos und Fotos an einen Mitschüler weiterleiteten, der sie auf Instagram verbreitet und teilweise mit sexistischen und beleidigenden Kommentaren versehen hat. Einer der beiden Minderjährigen hatte zugegeben, heimlich Bilder eines Lehrers im Unterricht angefertigt und an den Betreiber des Instagram-Accounts weitergeleitet zu haben. Der andere Schüler hatte jedenfalls nicht bestritten, genau dies auch getan zu haben. Die Schulleiterin hatte die beiden vorläufig für neun Schultage vom Unterricht suspendiert.

Nach Ansicht des VG war diese Sanktion rechtlich nicht zu beanstanden. Die Schulleiterin habe davon ausgehen dürfen, dass die Minderjährigen zumindest in Kauf genommen hätten, dass der Mitschüler das Bild- und Videomaterial auf seiner Instagram-Seite veröffentlichen und mit beleidigenden und sexistischen Inhalten versehen würde. Es sei lebensfremd anzunehmen, dass sie nicht gewusst hätten, was der Empfänger der Aufnahmen mit dem Bild- und Videomaterial machen würde, zumal einer der Schüler selbst einen solchen Account betreibe.

Darüber hinaus liege es auch auf der Hand, dass bei der hier nahe liegenden Weiterverbreitung und Kommentierung in den sogenannten sozialen Medien durch einen Mitschüler das „geordnete Schulleben beeinträchtigt werde“. Das Vertrauen der Schülerschaft in einen regelgeleiteten und friedlichen schulischen Rahmen sei „fortwährend erschüttert“ worden. Dies gelte in besonderem Maße, wenn die weiterverbreiteten Inhalte geeignet seien, die betroffenen Lehrkräfte in der Öffentlichkeit bloßzustellen. Die Entscheidung ist nicht rechtskräftig.

Neben der verwaltungsrechtlichen Frage nach der Zulässigkeit der Suspendierung droht in derartigen Fällen sogar strafrechtlicher Ärger. Zwar stellt ein Klassenraum keinen „höchstpersönlichen Lebensbereich“ dar, sodass eine Strafbarkeit des Filmens und Fotografierens im vorliegenden Fall ausscheidet. Allerdings schützt § 201 Strafgesetzbuch (StGB) vor der „Verletzung der Vertraulichkeit des Wortes“. Danach macht sich derjenige strafbar, der „das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt“ oder „eine so hergestellte Aufnahme einem Dritten zugänglich macht“. Dies dürfte auch für die Tonaufnahmen im Rahmen der Erstellung des Videos gelten. Daneben könnte der betroffene Lehrer auch aus Verletzungen seines Persönlichkeitsrechts sowie des Datenschutzrechts zivilrechtlich vorgehen, etwa durch Abmahnungen (Heidrich, Verwaltungsgericht bestätigt Suspendierung von Schülern wegen heimlicher Filmaufnahmen im Unterricht, www.heise.de 18.06.2019, Kurzlink: https://heise.de/-4449385).

VG Stuttgart

Verfassungsschutz Baden-Württemberg speicherte über Anwalt zu viel und zu lange

Mit Urteil vom 11.07.2019 hat die 1. Kammer des Verwaltungsgerichts (VG) Stuttgart über die Jahrzehnte andauernde Überwachung des Freiburger Rechtsanwalts (RA) Michael Moos durch das Landesamt für Verfassungsschutz Baden-Württemberg (LfV) entschieden (Az. 1 K 493/17). Moos führt seit 10 Jahren einen Kampf mit dieser Behörde um seine Daten. Das VG stellt in seiner Entscheidung fest, dass das LfV von Anfang an die Daten von 15 Verteidigerbesuchen von RA Moos in den Jahren 1982/3 bei einem inhaftierten Mandanten rechtswidrig erfasst und gespeichert hat, dass es die im Beobachtungsfeld „Linksterrorismus“ erhobenen Daten nicht länger als bis zum 31.12.1998 hätte speichern dürfen und dass die weitere Speicherung bis zur vom Verfassungsschutz selbst angeordneten Löschung am 07.02.2013 rechtswidrig gewesen ist. Das LfV hätte die von RA Moos im Beobachtungsfeld „Linksextremismus“ erhobenen Daten nicht länger als bis zum 31.12.2000 speichern dürfen. Die weitere Speicherung bis zur vom LfV selbst angeordneten Löschung am 07.02.2013 war somit auch rechtswidrig gewesen.

Es kommt äußerst selten vor, dass sich einE BürgerIn gegen die Beobachtung durch den Verfassungsschutz gerichtlich zu Wehr setzt. Dies ist nicht verwunderlich, denn die Betroffenen wissen in aller Regel gar nicht, dass sie vom Verfassungsschutz beobachtet und ihre Daten gespeichert werden. Und dann müssen sie Geduld, Energie und Kosten aufbringen, um vielleicht in einem jahrelangen Rechtsstreit, wie hier zumindest teilweise, zu obsiegen. Der Prozessbevollmächtigte von RA Moos, der Freiburger Rechtsanwalt und Vorsitzende der den Prozess unterstützenden Humanistischen Union Baden-Württemberg, Udo Kauß, kommentierte: „Diese Behörde ist es nicht gewohnt, dass ihr Handeln rechtlich und vor allem gerichtlich überprüft wird. Der Verfassungsschutz hat es sich in der Rolle eines ´rechtlich Unberührbaren` bequem gemacht. Und diese Behörde muss sich nun mit dem Vorwurf auseinandersetzen, über 14 Jahre hinweg rechtswidrig die Daten über einen Bürger gespeichert zu haben und damit die Hälfte aller über RA Moos gespeicherten Aktenseiten. Das sollte Konsequenzen haben. Es ist ein großer Fortschritt, dass der Verfassungsschutz sich nicht mit seiner Ansicht hat durchsetzen können, dass die Mitgliedschaft eines DKP-Funktionärs in der kommunalen Listenverbindung Linke Liste, der RA Moos im Freiburger Gemeinderat seit 1999 angehört, erlaubt, alle Personen, die mit diesem Funktionär in politischem Kontakt stehen, als linksextremistisch beeinflusst zu überwachen, wie dies im Fall von RA Moos geschehen ist.“

Weniger zufrieden zeigte sich Kauß über den Umstand, dass das Gericht die

Beobachtung und Speicherung von Daten über RA Moos für die Zeit von 1978 bis 1998 bzw. 2000 für rechtmäßig befunden hat. Er hatte sich im Umkreis einer vom LfV beobachteten angeblich linksextremistischen Organisation bewegt. Es kam nicht darauf an, dass RA Moos selbst keine verfassungsfeindlichen Bestrebungen verfolgte. Es reichte schon, wenn er – als eine Art Kontaktschuld – als Referent auf einer Veranstaltung z. B. der Roten Hilfe aufgetreten ist. Moos erläutert: „Da ich mich im Laufe der Jahrzehnte sehr häufig kritisch mit der Entwicklung vom Rechts- zum Sicherheitsstaat befasst habe und auf einer Vielzahl von Veranstaltungen dazu referiert und diskutiert habe, gibt es also eine Fülle von derartigen Erkenntnissen. Sogar das Einweihungsfest unserer Kanzlei im Hegar-Haus 1994 ist nachrichtendienstlich überwacht worden durch einen Spitzel des Amtes, eine ´Quelle`, wie es das Amt lieber hört. Ich wehre mich dagegen, dass meine Bemühen um rechtsstaatliche und demokratische Verhältnisse mit meiner Erfassung und Zuordnung zum ´linksterroristischen Beobachtungsfeld` quittiert wird" (Humanistische Union, LV Baden-Württemberg, PM im Rechtsstreit RA M. Moos, Freiburg ./. Verfassungsschutz BaWü, 12.07.2019).

AG Riesa

Gerechtfertigter Drohnenabschuss

Mit Urteil vom 24.04.2019 wurde vom Amtsgericht (AG) Riesa ein wegen Sachbeschädigung Angeklagter freigesprochen. Er hatte eine fremde Kameradrohne abgeschossen, die unerlaubt über sein Grundstück flog (Az.: 9 Cs 926 Js 3044/19). Der Angeklagte hielt sich am Tattag im Garten seines Grundstücks auf, das von einer hohen Hecke umgeben ist. Während er in der Garage beschäftigt war, stellte seine Frau fest, dass eine Drohne über dem Grundstück flog und ihre Bewegungen verfolgte. Auch die beiden drei- und siebenjährigen Töchter hätten sich von dem Flugobjekt bedroht gefühlt und seien aufgelöst zu ihrer Mutter gelaufen. Der Drohnenpilot meinte, er könne nicht ausschließen, das Grundstück überflogen zu haben. Er habe wegen des Überflugs sich selbst angezeigt, ein Bußgeldverfahren sei anhängig. Die Drohne flog etwa in der Mitte des Grundstücks des Angeklagten in einer Höhe zwischen 5 bis 15 Meter. Er rief zunächst laut, dass das Gerät entfernt werden solle und ging dann ins Haus, um sein Luftgewehr zu holen. Der für den Schützen nicht erkennbare Pilot reagierte darauf jedoch nicht. Mit dem zweiten Diabolo-Projektil traf der Angeklagte die Drohne, die dann auf das Garagendach des Angeklagten fiel und dabei vollständig zerstört wurde. Die 40 cm x 40 cm große und mit Kamera ausgestattete Drohne konnte aus einer Distanz von bis zu einem Kilometer gesteuert werden und kostete rund 1.500 €. Ihr Eigentümer hatte Strafantrag wegen Sachbeschädigung gestellt. Die Staatsanwaltschaft nahm zudem ein besonderes öffentliches Interesse an der Strafverfolgung nach § 303c Strafgesetzbuch (StGB) an.

Das AG sprach den Angeklagten von dem Vorwurf der Sachbeschädigung frei. Er habe gemäß § 228 Bürgerliches Gesetzbuch (BGB), dem so genannten Defensivnotstand, gerechtfertigt gehandelt. Danach gilt, dass, wer eine fremde Sache beschädigt oder zerstört, um „eine durch sie drohende Gefahr von sich oder einem anderen abzuwenden", nicht widerrechtlich handelt. Dies gilt zumindest dann, wenn die Beschädigung oder die Zerstörung erforderlich ist, um eine Gefahr abzuwenden und der Schaden nicht unverhältnismäßig ist. Der Drohnenbesitzer habe mit dem Überflug das allgemeine Persönlichkeitsrecht verletzt. Dieses Recht gewährt das Recht, die Darstellung der eigenen Person anderen gegenüber selbst zu bestimmen. Wer in diesen privaten Bereich eindringt, verletze als „Ausspähung" das allgemeine Persönlichkeitsrecht. Erschwerend komme im vorliegenden Fall hinzu, dass bei Drohnenaufnahmen die betroffene Person diese gar nicht mitbekommt, da sie nicht mit einer Aufnahme „von oben" rechnet. Dies hatte bereits das AG Potsdam in einem Urteil vom 16.04.2015 entschieden (Az.: 37 C 454/13).

Umgekehrt geht das AG davon aus, dass der Drohnenpilot den „höchstpersönlichen Lebensbereich durch Bildaufnahmen" verletzt habe (§ 201a StGB). Danach wird unter anderem bestraft, wer von einer anderen Person, die sich in einem gegen Einblick besonders geschützten Raum befindet, unbefugt eine Bildaufnahme herstellt oder überträgt. Hierunter falle auch ein gegen Einsicht besonders geschützter Garten, ebenso wie Echtzeitübertragungen, ohne die dauernde Speicherung der aufgenommenen Bilder. Zudem sei durch das niedrige Überfliegen des Gartens ohne Einverständnis auch das Eigentum des Angeklagten verletzt worden. Nach § 21b der Luftverkehrs-Ordnung (LuftVO) ist der Betrieb von unbemannten Luftfahrtsystemen und Flugmodellen über Wohngrundstücken verboten, wenn die Startmasse des Geräts mehr als 0,25 kg beträgt oder das Gerät in der Lage ist, „optische, akustische oder Funksignale zu empfangen, zu übertragen oder aufzuzeichnen". Eine Ausnahme kennt das Gesetz nur dann, wenn der betroffene Eigentümer dem Überflug zustimmt, was der Angeklagte oder seine Frau explizit nicht getan haben. Da allerdings kein Strafantrag gestellt worden war, kam der Pilot ohne Verurteilung davon. Die AG-Entscheidung ist jedoch kein Persilschein für schießwütige Drohnenopfer. Grundsätzlich kann in einer vergleichbaren Situation auch ein milderes Mittel zumutbar sein, wie etwa die Flucht. Schon durch das „Verfolgen" der Frau des Angeklagten sowie die geringe Höhe des Fluges sei im vorliegenden Fall aber eine deutlich über eine bloße Lästigkeit hinausgehende Intensität erreicht, die einen Abschuss der Drohne rechtfertigte (Heidrich, Abschuss fremder Kameradrohne über eigenem Grundstück kann gerechtfertigt sein, www.heise.de 27.06.2019, Kurzlink: https://heise.de/-4456039).

OVG NRW

Auskunftsverweigerung an Pau und Ramelow war rechtswidrig

Das für Nordrhein-Westfalen (NRW) zuständige Oberverwaltungsgericht Münster (OVG) hat mit Urteilen vom 31.07.2019 entschieden, dass das Bundesamt für Verfassungsschutz

(BfV) über die Auskunftsanträge des Thüringer Ministerpräsidenten Bodo Ramelow und der langjährigen Bundestagsvizepräsidentin Petra Pau betreffend die Akte zur Partei Die Linke neue Entscheidungen treffen muss (16 A 1009/14 1. Instanz: VG Köln 20 K 6112/09; 16 A 1010/14, 1. Instanz: VG Köln 20 K 6717/12). Das BfV hatte den Klägern die Auskunft darüber verweigert, welche Daten zu ihren Personen in der dortigen Sachakte zur Partei Die Linke enthalten sind. Der 16. Senat des OVG begründete seine Urteile damit, dass die Ablehnung der begehrten Auskunft rechtswidrig gewesen sei, weil das BfV sein Ermessen nicht ordnungsgemäß ausgeübt habe. Es kann sich weder auf Ausforschungsgefahren berufen, noch reicht ein pauschaler Verweis auf den Verwaltungsaufwand einer Auskunft für die Ablehnung.

Ramelow und Pau, die beide der Linkspartei angehören, kämpfen seit Jahren darum zu erfahren, was der Verfassungsschutz alles über sie gesammelt hat. Das Verwaltungsgericht (VG) Köln hatte den beiden bereits vor Jahren Recht gegeben. Doch das BfV weigerte sich bisher und erklärte, man könne die Akten nicht herausgeben, weil man sonst erkennen könne, nach welchen Kriterien das Amt die Partei Die Linke beobachte. Ramelow hat auch schon das Bundesverfassungsgericht angerufen, das im Jahr 2013 feststellte, dass seine Überwachung verfassungswidrig gewesen sei. Dabei wurden hohe Hürden für die Beobachtung von Parlamentariern definiert. In einem mehr als 50-seitigen Schriftsatz hatte das BfV erklärt, es könne keinesfalls sogenannte Sachakten herausgeben, lediglich Personenakten, die über eine bestimmte Person angelegt wurden, aber auch die nur geschwärzt. Allein der Name Petra Pau tauche von 2007 bis 2012 mehr als 400 Mal in den Akten auf. Diese zu sichten sei zu aufwändig. Gleichzeitig hieß es, die Akten würden nicht mehr genutzt und seien innerhalb des Amtes vor jedem Zugriff durch Mitarbeitende geschützt. Am Ende des Verfahrens erklärte die Richterin, man könne nicht mehr erkennen, was denn nun die Wahrheit sei.

Pau erklärte nach dem Urteil: „Ich erwarte nun Nachricht vom Bundesamt. Ich bin gespannt, was sich das Bundesamt einfallen lässt, um mir wieder keine Einsicht zu gewähren." Die Bundestagsvizepräsidentin, die seit 21 Jahren im Parlament sitzt, will ihre Akteneinsicht bis zum Ende durchfechten. Sie meint, die Unterlagen müssten längst ins Bundesarchiv überstellt werden, als zeitgeschichtliches Dokument, und von Wissenschaftlern erforscht werden können. Das Archivrecht sieht vor, dass der Verfassungsschutz nicht mehr benötigte Akten dem Bundesarchiv anbieten muss. Dies ist aber in Sachen Pau und Ramelow nicht geschehen. Das OVG hat die Revision gegen die Urteile nicht zugelassen. Dagegen kann Nichtzulassungsbeschwerde erhoben werden, über die das Bundesverwaltungsgericht entscheidet (Bundesamt für Verfassungsschutz muss über Auskunftsbegehren von Bodo Ramelow und Petra Pau erneut entscheiden, http://www.ovg.nrw.de, PE 31.07.2019; Ramelsberger, Verfassungsschutz muss Einblick geben, SZ 01.08.2019, 6).

VG Wiesbaden

Keine Herausgabe der BKA-„Feindesliste"

Das Bundeskriminalamt (BKA) muss von Rechtsextremisten zusammengestellte Namenslisten weiterhin nicht veröffentlichen. Ein Verfahren vor dem Verwaltungsgericht (VG) Wiesbaden wurde am 19.08.2019 nach einstündiger mündlicher Verhandlung eingestellt, nachdem beide Parteien die Sache für erledigt erklärt hatten (Az. 6 K 376/19 WI). Ein Journalist und Aktivist hatte unter Berufung auf das Informationsfreiheitsgesetz des Bundes (IFG) die Herausgabe von der als „Feindesliste" bekannt gewordenen Datensammlung erzwingen wollen. Rund 25.000 Namen stehen insgesamt auf diversen Listen, die Ermittler bei Razzien gegen rechte Extremisten und sogenannte Prepper 2017 und 2018 gefunden hatten. Prepper bereiten sich auf den Zusammenbruch der staatlichen Ordnung vor, es gibt Überschneidungen mit Reichsbürgern und Rechtsextremisten. Der Mitarbeiter des Portals „FragDenStaat" hatte das BKA aufgefordert, die Namenslisten zu veröffentlichen. Die Behörde hatte ihm das mehrfach verweigert. Vor Gericht beriefen sich BKA-Vertreter auf ein laufendes Ermittlungsverfahren beim Generalbundesanwalt (GBA) und erklärten sich für nicht zuständig. Der Anwalt des Klägers zeigte sich verwundert: Seit 2018 korrespondiere der Aktivist mit der Behörde; vom GBA sei nie die Rede gewesen.

Richter Hans-Hermann Schild erläuterte in der mündlichen Verhandlung, dass kein Anspruch auf Herausgabe nach dem IFG besteht, wenn das BKA im Auftrag der Staatsanwaltschaft handelt und die Listen Teil eines laufenden Ermittlungsverfahrens sind. Er regte eine Einigung zwischen den Parteien an, da sich das BKA erst jetzt qualifiziert zu der Liste geäußert habe. Hätte es die Informationen dem Journalisten schon im behördlichen Vorverfahren mitgeteilt, hätte dieser wohlmöglich auf eine Klage verzichtet. Beide Parteien müssen nun die Hälfte der Verfahrens- und Gerichtskosten tragen. Das BKA erklärte, ein Großteil der Namen stamme aus einer 2015 gehackten Kundendatei eines Online-Händlers, die als „Antifa-Liste" tituliert wurde. Weitere, kleinere Datensätze stammten von Mitgliedern von Gruppierungen wie den „Nordkreuz"-Preppern. Die Summe aller Namen auf allen Datenträgern betrage ca. 25.000; eine „Feindesliste" sei das aber nicht.

Kläger Arne Semsrott sieht die Niederlage dennoch als Erfolg. Der öffentliche Druck sei inzwischen so groß, dass sich etwas bewege: „Das BKA schiebt die Verantwortung für den Umgang mit den Listen von sich. Aber wir werden eine Stelle finden, die sich verantwortlich fühlt." Nach den Auskünften aus dem Verfahren dürfte die Suche schnell beim GBA enden. Richter Schild gab dem Journalisten noch mit auf den Weg, es doch lieber mit dem presserechtlichen Auskunftsanspruch zu versuchen: „Da haben Sie viel größere Chancen" (BKA muss „Feindesliste" nicht veröffentlichen, www.lto.de 19.08.2019).



SO WIE ES JETZT AUSSIEHT, ZEICHNET SICH EIN HARTER BREXIT AB. DAMIT WÄRE GROSSBRITANNIEN IN PUNKTO DATENSCHUTZ EIN UNSICHERES DRITTLAND.

ICH DENKE, WIR SOLLTEN UNS KEINE VOREILIGEN SORGEN MACHEN. DONALD TRUMP IST ZWAR MIT SEINEM VERSUCH, GRÖNLAND ZU KAUFEN, GESCHEITERT, ABER VIELLEICHT MACHT ER JETZT DEM VEREINIGTEN KÖNIGREICH EIN TOLLES ANGEBOT. DANN HÄTTEN WIR BEI EINER ANNAHME DES DEALS WIEDER RECHTSSICHERHEIT.

Bild: Frans Valenta